ConneXium
Ethernet Cabling System
Managed Switch
Configuration Manual

8/2006

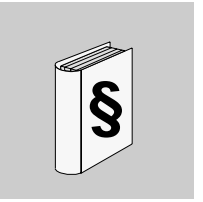
Clipsal
Merlin Gerin
Square D
TAC
Telemecanique

Schneider Electric
Building a New Electric World

31007122.01

Table of Contents

Safety Information



Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation, which, if not avoided, **will result** in death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation, which, if not avoided, **can result** in death, serious injury, or equipment damage.

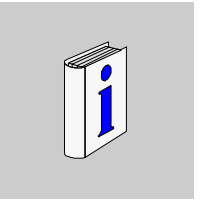
⚠ CAUTION

CAUTION indicates a potentially hazardous situation, which, if not avoided, **can result** in injury or equipment damage.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

About the Book



At a Glance

Document Scope

The Schneider Electric ConneXium Industrial Ethernet Offer is comprised of a complete family of products and tools required to build the infrastructure of an Industrial Ethernet network.

The offer includes:

- switches, hubs, and transceivers
- gateways
- cables, connectors, and accessories

This manual contains a device description, safety instructions, technical data and all the other information you need to install the ConneXium ESM Ethernet switches before you start configuring them. This manual contains all the information you need to choose and configure the appropriate redundancy procedures for a ConneXium ESM Ethernet switch.

Validity Note

The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

Related Documents

Title of Documentation
ConneXium Ethernet Cabling System Managed Switch Redundancy Manual
ConneXium Ethernet Cabling System Managed Switch Command Line Interface
ConneXium Ethernet Cabling System Managed Switch Installation Manual

Product Related Warnings

Schneider Electric assumes no responsibility for any errors that may appear in this document. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

When controllers are used for applications with technical safety requirements, please follow the relevant instructions.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this product related warning can result in injury or equipment damage.

User Comments

We welcome your comments about this document. You can reach us by e-mail at techpub@schneider-electric.com

The User Interfaces

1

At a Glance

Overview

This chapter provides information concerning the user interfaces.

What's in this Chapter?

This chapter contains the following topics:

The System Monitor

Features of the System Monitor

The System Monitor enables you to

- select the boot operating system,
- update the operating system,
- start the selected operating system,
- end the System Monitor,
- erase the saved configuration, and
- show the boot code information.

Data Transfer Parameters

The following table shows the data transfer parameters.

Parameter	Value or Status
Speed	9600 baud
Data	8 bit
Parity	none
Stopbit	1 bit
Handshake	off

Opening the System Monitor

Open and the System Monitor as follows:

Step	Action	Comment
1	Connect the V.24 RJ11 socket to • either a terminal • or a COM port of a PC with terminal emulation according to VT 100 using a terminal cable.	The V.24 interface of the switch supports the baud rates 9600 and 19200 (default setting: 9600). For the physical connection refer to the **Installation User Manual**.
2	Start the terminal program on the PC, and establish a connection with the switch.	While the ESM is being booted, the following message appears on the terminal: **Press <1> to enter System Monitor 1...**
3	Type `1` within one second to start System Monitor 1.	Subsequently, System Monitor 1 displays the following information: **1. Select Boot Operating System** **2. Update Operating System** **3. Start Selected Operating System** **4. End (reset and reboot)** **5. Erase main configuration file** **6. Show Bootcode Information**
4	Select the desired menu by typing its number.	
5	To leave a sub menu and to return to the main menu of the System Monitor, press **ESC**.	

The Command Line Interface (CLI)

Features of the CLI

The CLI allows you to

- use all device functions via a local or remote connection,
- provides you with a familiar environment for configuring IT devices,
- feed several devices with identical configuration data, due to its script ability.

For a detailed description of the CLI, refer to the reference guide **Command Line Interface**.

Interfaces to Access the CLI

The CLI can be accessed using

- the V.24 port (out-of-band) or
- Telnet (in-band).

Abbreviating Keywords

In the CLI, you can abbreviate keywords as follows:

Step	Action	Comment
1	Type the first letters of the keyword.	
2	Press the TAB key.	The command line interface adds the remaining letters for you.

Opening the CLI

Open the CLI as follows:

Step	Action	Comment
1	Connect the device via the V.24 interface to • a terminal • or to a COM port of a PC with terminal emulation according to VT 100 using a serial cable, and press any key (see *p. 13*), or start the CLI using Telnet.	A window in which you are asked to enter your user name appears on the screen. (A maximum of five users are permitted to access the CLI).
2	Type a user name.	The default setting for the user name is **admin**. You can change the user name later in the CLI. Note that these entries are case sensitive.
3	Press the ENTER key.	
4	Type the password.	The default setting for the password is **private**. You can change the password later in the CLI. Note that these entries are case sensitive.
5	Press the ENTER key.	

The Web-Based Interface

Requirements

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example, Netscape Navigator/Communicator version 6.0 or higher or Microsoft Internet Explorer version 5.5 or higher.

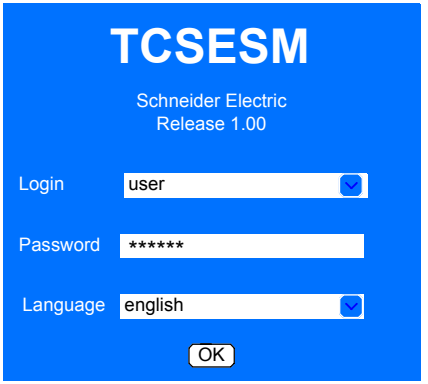
Enabling the Web-Based Interface

The following table shows the steps to enable the Web-based interface.

Step	Action	Comment
1	Connect the ESM switch to an Ethernet cable.	
2	Start your Web browser.	
3	Make sure that Java Script is active on your browser.	
4	Establish the connection by entering the IP address of the switch with which you want to administer the Web-based network management in the address field of the Web browser. Enter the address in the following form: `http://xxx.xxx.xxx.xxx`	The Web-based interface uses the plug-in Java™ runtime environment version 1.4. If this is not installed on your computer, an installation via the Internet starts automatically the first time you start the Web-based interface. If your computer is not connected to the Internet, or you do not have access to the Java plug-in, install the version on the enclosed CD-ROM. **For NT users and computers not connected to the Internet**: Cancel the installation and install the plug-in from the enclosed CD-ROM. Start the program file **j2re1_4_0-win-i.exe** in the *Java* directory on the CD-ROM.

Login Screen

The figure below shows the login window.



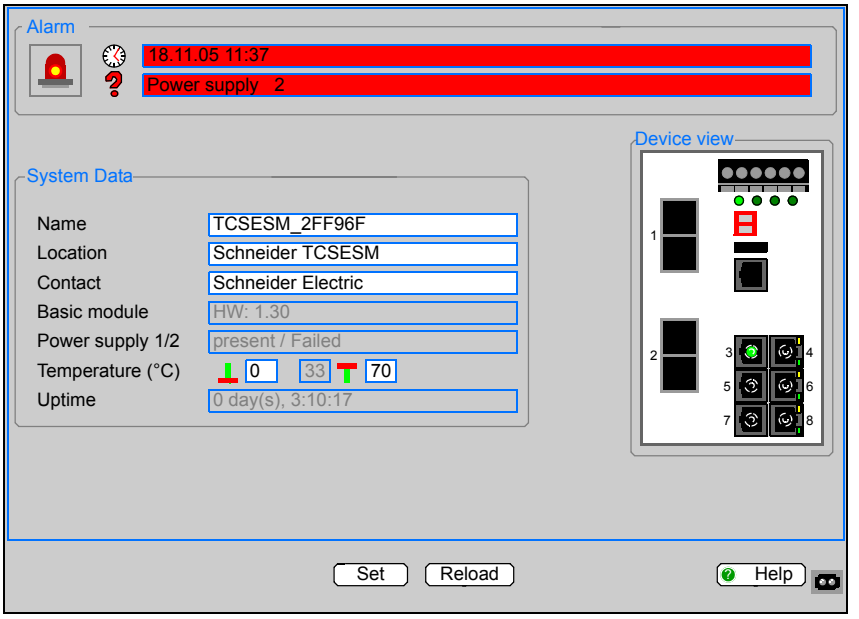
Logging In

Log in as follows:

Step	Action	Comment
1	Select the desired language.	Choose **english** or **german**.
2	In the **login** pull-down menu, select either **user** or **admin** access to access the switch.	**user**: read access **admin**: read and write access
3	For read permission, enter the password **public**. For read/write permission, enter the password **private** (default setting).	Change the password from these default settings to protect the switch against unauthorized access.
4	Click **OK**.	The system screen appears.

System Screen

The figure shows the system screen of the ESM switch.



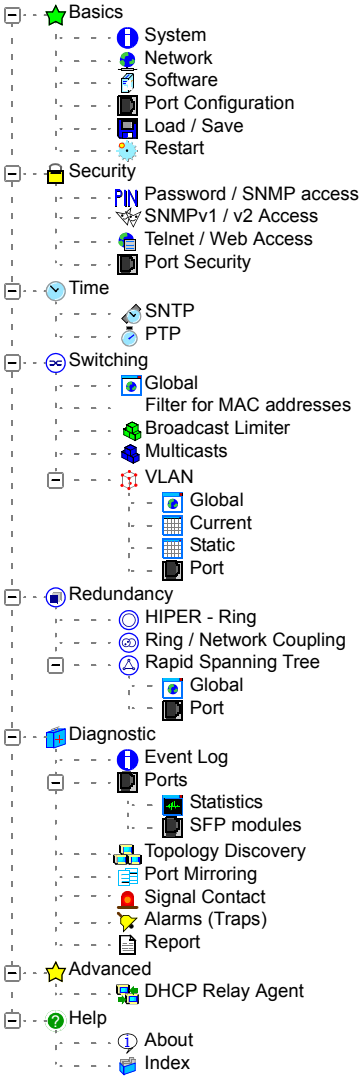
The Set and Reload Buttons

The table explains the **Set** and **Reload** buttons.

Set	**Reload**
Click the **Set** button to save the changes you have made to the dialogs.	Click the **Reload** button to update the system screen.

The Tree View

The figure below shows the tree view of the Web-based interface. All path references in the manual refer to this tree view. For example: Go to **Basics** → **System**.



Entering the IP Parameters

2

At a Glance

Overview

This chapter provides information concerning the IP parameters.

What's in this Chapter?

This chapter contains the following topics:

Basics of the IP Parameters

Background Information concerning the IP Address

The IP address is used for the configuration of the ESM. The IP address background information is discussed here.

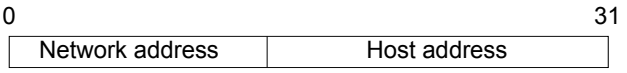
The IP addresses consist of four bytes. These four bytes are written in decimal notation, each separated by a dot. Five classes of IP addresses were defined in RFC 790 (1992). The most frequently used address classes are A, B and C.

The following table describes IP address classification.

Class	Net Address	Host Address	Address Range
A	1 byte	3 bytes	1.0.0.0 to 126.255.255.255
B	2 bytes	2 bytes	128.0.0.0 to 191.255.255.255
C	3 bytes	1 bytes	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

The network address, assigned by ARIN (American Registry for Internet Numbers), represents the fixed part of the IP address.

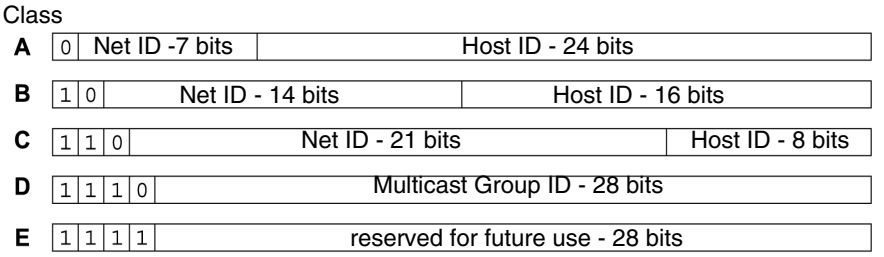
The following figure shows the bit notation of the IP address.



The network address represents the fixed part of the IP address. The worldwide leading regulatory board for assigning Internet addresses is the IANA (Internet Assigned Numbers Authority). If you need an IP address block, contact your Internet service provider. Internet service providers should contact their local higher level organization:

- APNIC (Asia Pacific Network Information Centre): Asia/Pacific region
- DARIN (American Registry for Internet Numbers): Americas and Sub-Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry): Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens): Europe and Surrounding Regions

The bit representation of the IP address is shown in the following figure.



All IP addresses belong to class A when their first bit is a zero, i.e., the first decimal number is 126 or less.

The IP address belongs to class B if the first bit is 1 and the second bit is 0, i.e., the first decimal number is between 128 and 191.

The IP address belongs to class C if the first two bits are a 1, i.e., the first decimal number is higher than 191.

Assigning the host address (host ID) is the responsibility of the network operator, who is solely responsible for the uniqueness of the assigned IP addresses.

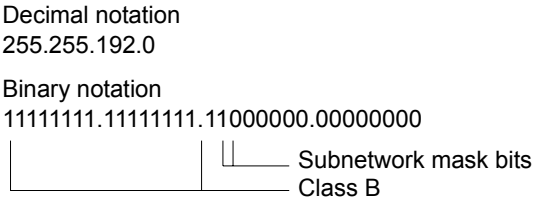
Network Mask

Routers and gateways subdivide large networks into subnetworks. The network mask assigns the individual devices to particular subnetworks.

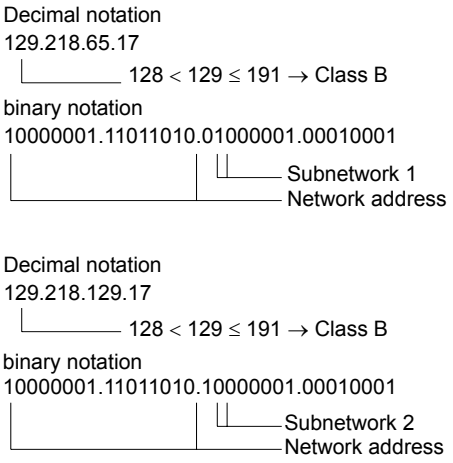
The subdivision of the network into subnetworks is performed in much the same was as IP addresses are divided into classes A to C (net ID).

The bits of the host address (host ID) that are to be shown by the mask are set to one. The other host address bits are set to zero in the network mask (see the following example).

The following figure shows an example of a network mask.



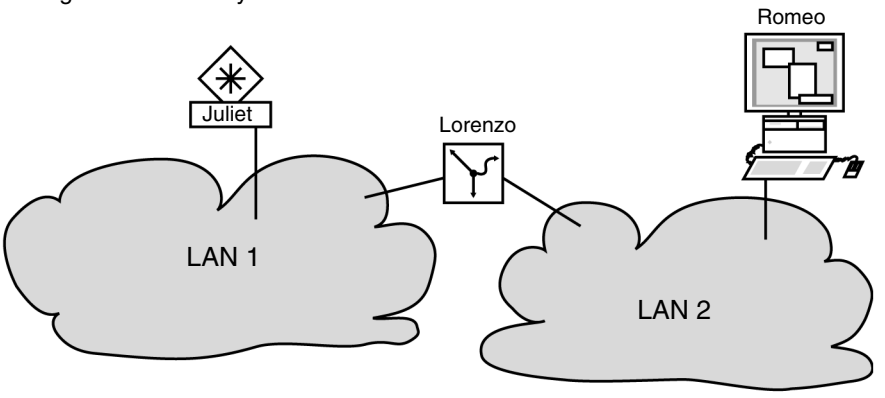
The following figure shows an example of IP addresses with subnetwork allocation in accordance with the network mask from the above example.



Example of Network Mask Usage

In a large network it is possible that gateways and routers separate the management card from its management station. How does addressing work in such a case?

The figure below shows a management agent that is separated from its management station by a router.



Sending Data

The management station **Romeo** wants to send data to the management agent **Juliet**. Romeo knows Juliet's IP address and also knows that the router **Lorenzo** knows the way to Juliet.

Example

Romeo therefore puts his message in an envelope and writes Juliet's IP address on the outside as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer three to layer two of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer two to layer one, i.e., to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope, exposing the inner envelope with Romeo's IP address. Opening the letter and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. The question then arises, where should she send the letter, since she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable **aNetGatewayIPAddr** as a means of communicating with Romeo. The envelope with the IP addresses is therefore placed in a further envelope with the MAC destination address of Lorenzo.

The letter then travels back to Romeo via Lorenzo, in the same manner that the first letter traveled from Romeo to Juliet.

Configuring the ESM using the Command Line Interface

General Information concerning the Configuration via CLI

Choose this method if

- you preconfigure your switch outside its operating environment, or
- if you have no network access to the switch.

Note: If there is no terminal or PC with terminal emulation available in the vicinity of the installation location, you can also enter the IP parameters in your working environment prior to performing the ultimate installation.

Entering the IP Parameters Using the CLI

Enter the IP parameters using the CLI as follows:

Step	Action	Comment
1	Establish a connection to the switch, following the instructions made in the step action table on *p. 15*.	
2	Change to the privileged EXEC mode by entering `enable`, and press ENTER.	
3	Enter the password, and press ENTER.	Press ENTER without typing the password, since the default setting is **no password**.
4	Disable DHCP by typing `network protocol none`, and press the ENTER key.	

Step	Action	Comment
5	Enter the following IP parameters: **IP address network mask** and, if necessary, **gateway**	• Local IP Address The default setting local IP address of the switch is 0.0.0.0. • Network Mask Enter the networks mask here if your network has been divided into subnetworks, and if these are identified with a network mask. The default setting of the network mask is 0.0.0.0. • IP Address of the Gateway This entry is only needed if the switch and the management station/tftp server are located in different subnetworks. Type the IP address of the gateway between the subnetwork of the switch and the path to the management station. The default setting of the IP address is 0.0.0.0.
6	Save the configuration entered by typing the command `copy system:running-config nvram:startup-config`, and press ENTER.	
7	Confirm that you wish to save by pressing Y.	

Configuring the Switch Using the Web-Based Interface

After entering the IP parameters using the CLI, you can easily configure the ESM using the Web-based interface (see *p. 41*).

Configuring the ESM Using the Ethernet Switch Configurator (ESC) Software

General Information

Select the IP address using the ESC software if

- the ESM is already installed on your network, or
- if there is another Ethernet connection between your PC and the ESM available.

Note: You can easily configure additional parameters using the Web-based interface (see *p. 41*).

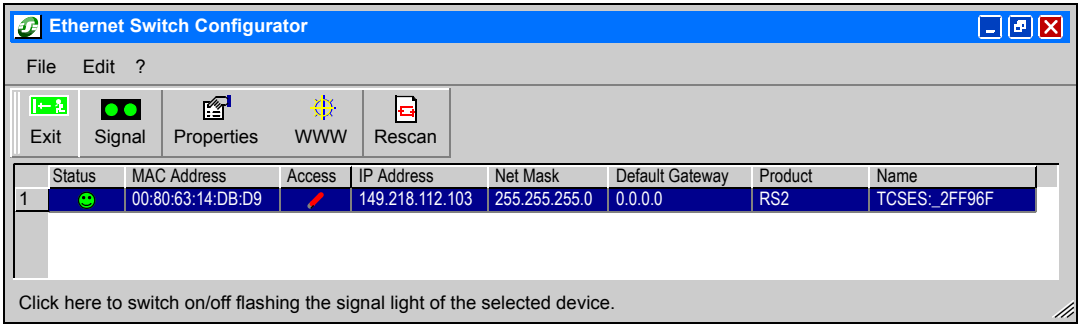
Note: The installation of the ESC involves installing the version 3.0 of the WinPcap software package.
If an earlier version of WinPcap is already installed on the PC, you must uninstall it first. A newer version remains intact when you install the Ethernet Switch configurator. However, this cannot be guaranteed for all future versions of WinPcap. If the installation of the ESC has overwritten a newer version of WinPcap, you must uninstall WinPcap 3.0 and then reinstall the new version.

Installing the ESC Software

Install the WinPcap software on your PC as follows:

Step	Action
1	To install the ESC software on your PC, start the installation program on the CD supplied with the switch, and follow the instructions given by the program.
2	Start the ESC program. Subsequently, the screen displayed below appears.

This figure shows the start screen of the ESC.



General Information concerning the ESC Software

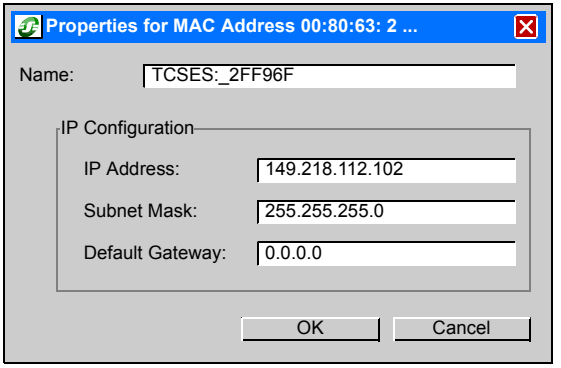
When the ESC software is started, it automatically searches the network for devices supporting the ESC protocol.

The ESC program uses the first PC network card found. If your computer has more than one network card, you can select them on the toolbar of the ESC program.

The ESC program displays a line for each device which responds to the ESC protocol.

Configuring your ESM Using the ESC

Configure the ESM as follows:

Step	Action
1	Select the device line of the ESM.
2	Click the symbol with the two green dots in the toolbar to set the LEDs for the selected device flashing. To switch off the flashing, click the symbol again.
3	Double-click the device line of your switch to open the window displayed below: In this dialog you can enter your device name as well as the IP parameters. 
4	Enter your device name as well as your IP parameters.
5	For security reasons, switch off the ESC function for the device in the Web-based interface after you have assigned the IP parameters to the device (see *p. 70*).
6	Save the settings you have made so they will still be available after restart (see *p. 50*).

Note: After the IP address has been entered and saved, the ESM loads the local configuration settings (see *p. 44*).

Loading the System Configuration from the Memory Back Up Adapter (EAM)

Uses of the EAM

The EAM is a USB device used for

- storing the configuration data of an ESM,
- storing the ESM software,
- providing back-up if the ESM fails.

Loading the System Configuration from the EAM

In case the switch fails, the EAM enables a very simple configuration data transfer by means of a substitute switch of the same type.

When you start the switch, it checks for an EAM. If it detects an EAM with a valid password and valid software, the ESM loads the configuration data from the EAM.

The password is valid if

- the password on the ESM matches the password on the EAM, or
- the default password is saved on the ESM.

To save the configuration data in the EAM, see *p. 50*.

Loading the System Configuration from the Local Memory

Note: If there is no valid password, load the system configuration from the local memory.

System Configuration Using BOOTP

Basic Information

To configure the ESM using BOOTP, you need a BOOTP server. The BOOTP server matches the configuration data to the ESM on the basis of its MAC address.

Note: For loading the configuration data, the ESM default setting is **DHCP mode**, so this method requires changing the ESM to the BOOTP mode.

Configuration Procedure Using CLI or the Web-Based Interface

Configure the ESM as follows:.

Step	Action
1	Activate BOOTP to receive the configuration data in the CLI, or refer to *p. 41*.
2	Change to the privileged EXEC mode by typing `enable`, and press the ENTER key.
3	Enable BOOTP by typing `network protocol BOOTP`, and press the ENTER key.
4	Perform the configuration, providing the BOOTP server with the switch data listed in the block **ESM Data for BOOTP Server** below.
5	Save the configuration performed by typing the command `copy system:running nvram:startup-config`, and press the ENTER key.
6	Confirm that you wish to save the configuration by pressing Y.

ESM Data for BOOTP Server

Provide the BOOTP server with the following ESM data:

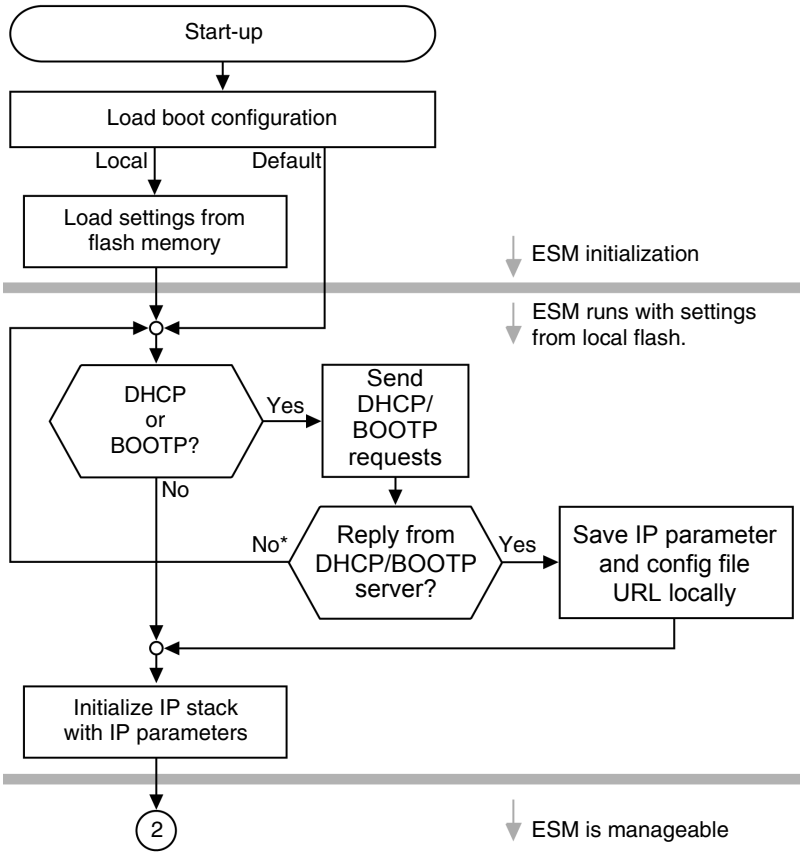
```
# /etc./bootptab for BOOTP-daemon bootpd
#
# gw -- gateways
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template
```

.global:/
:gw=0.0.0.0:/
:sm=255.255.240.0:
rs2:01:ht=ether
net:ha=008063086501:ip=149.218.17.83:tc=.global:
rs2_02:ht=ether-
net:ha=008063086502:ip=149.218.17.84:tc=.global:

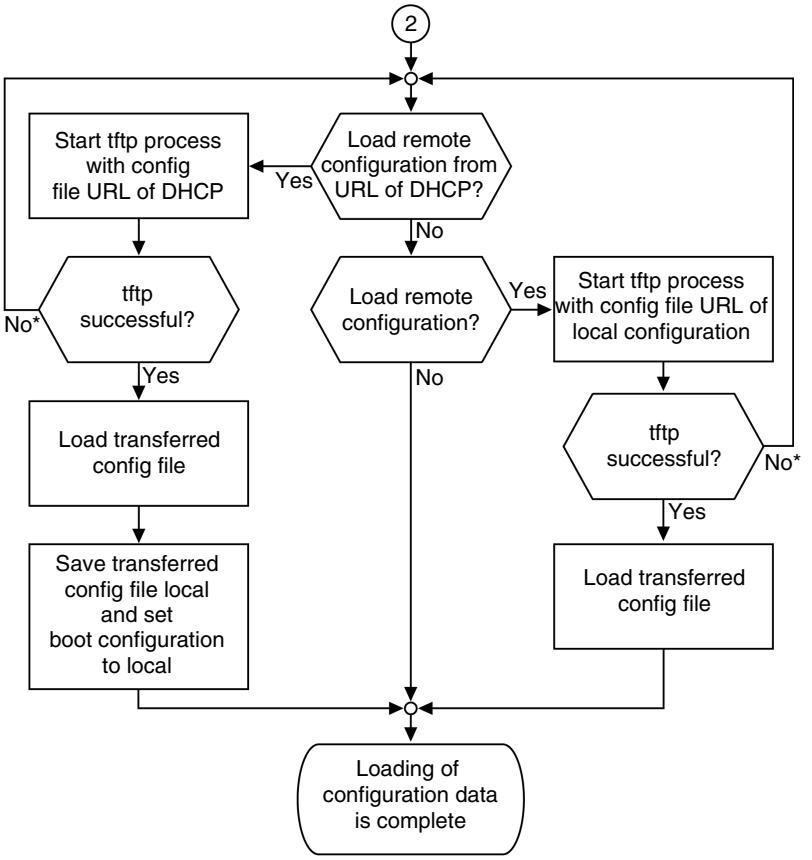
Note: Lines that start with a # character are comment lines. The lines under **global** make the configuration of several devices easier. The template (tc) allows you to allocate the global configuration data (tc=.global:). The direct allocation of the hardware or IP address occurs in the device lines (rs2-0).

Flow Chart for the BOOTP Process

This figure illustrates the BOOTP process.



The following figure shows part 2 of the BOOTP/DHCP process.



Note: The agent of the ESM does not support IEEE 802.3 frame type.

System Configuration Using DHCP

General Information

To configure the system via DHCP (Dynamic Host Configuration Protocol), you need a DHCP server. The DHCP server matches the configuration data to the ESM on the basis of its MAC address or its system name.

The DHCP (responds similar to the BOOTP and offers in addition the configuration of a DHCP client with a name instead of the MAC address. For the DHCP, this name is known as the client identifier in accordance with rfc 2131.

The ESM uses the name entered under `sysName` as the client identifier in the system group of the MIB II. You can enter the system name directly via SNMP, the Web-based management or the user interface.

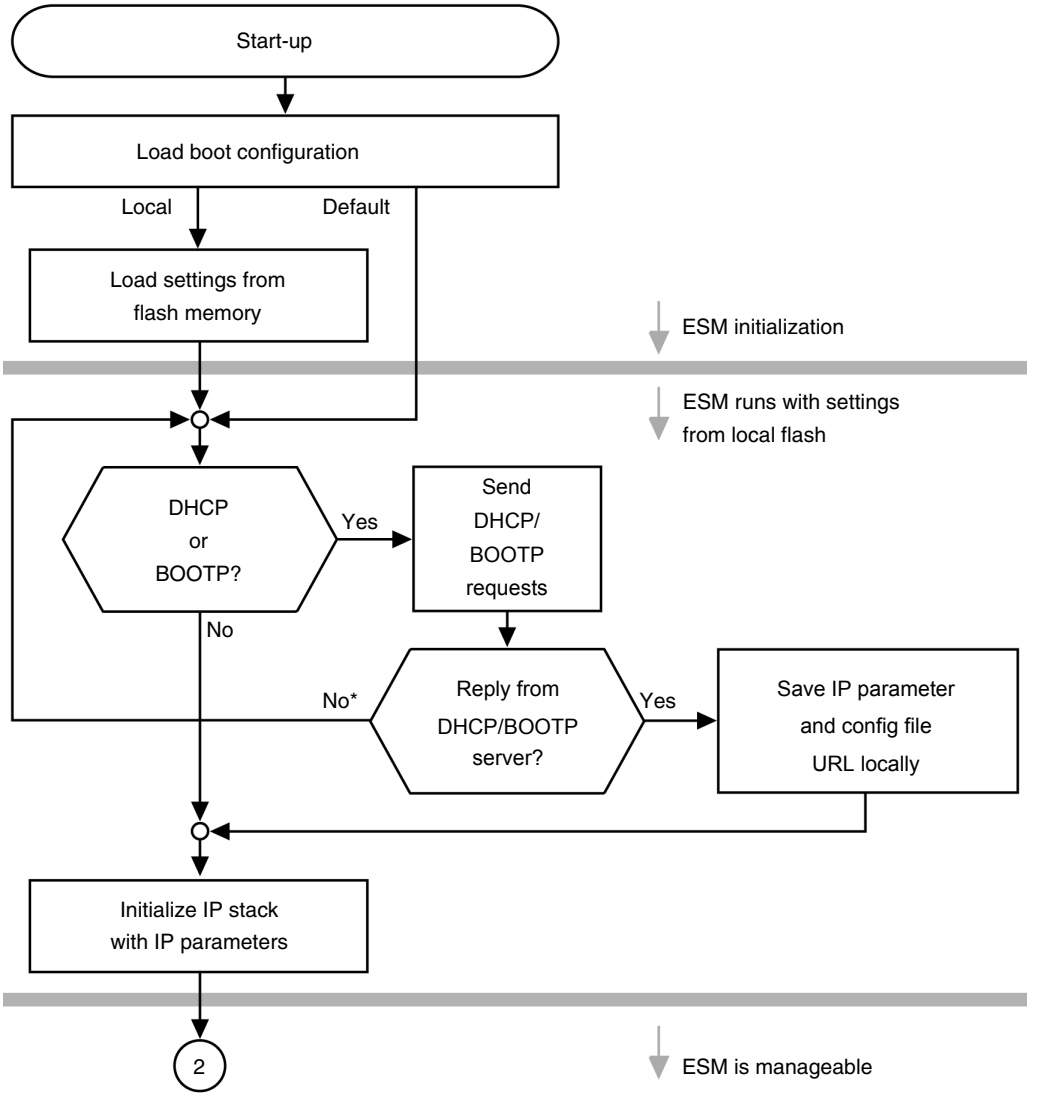
Configuration Procedure Using the CLI or the Web-Based Interface

Configure the ESM as follows:

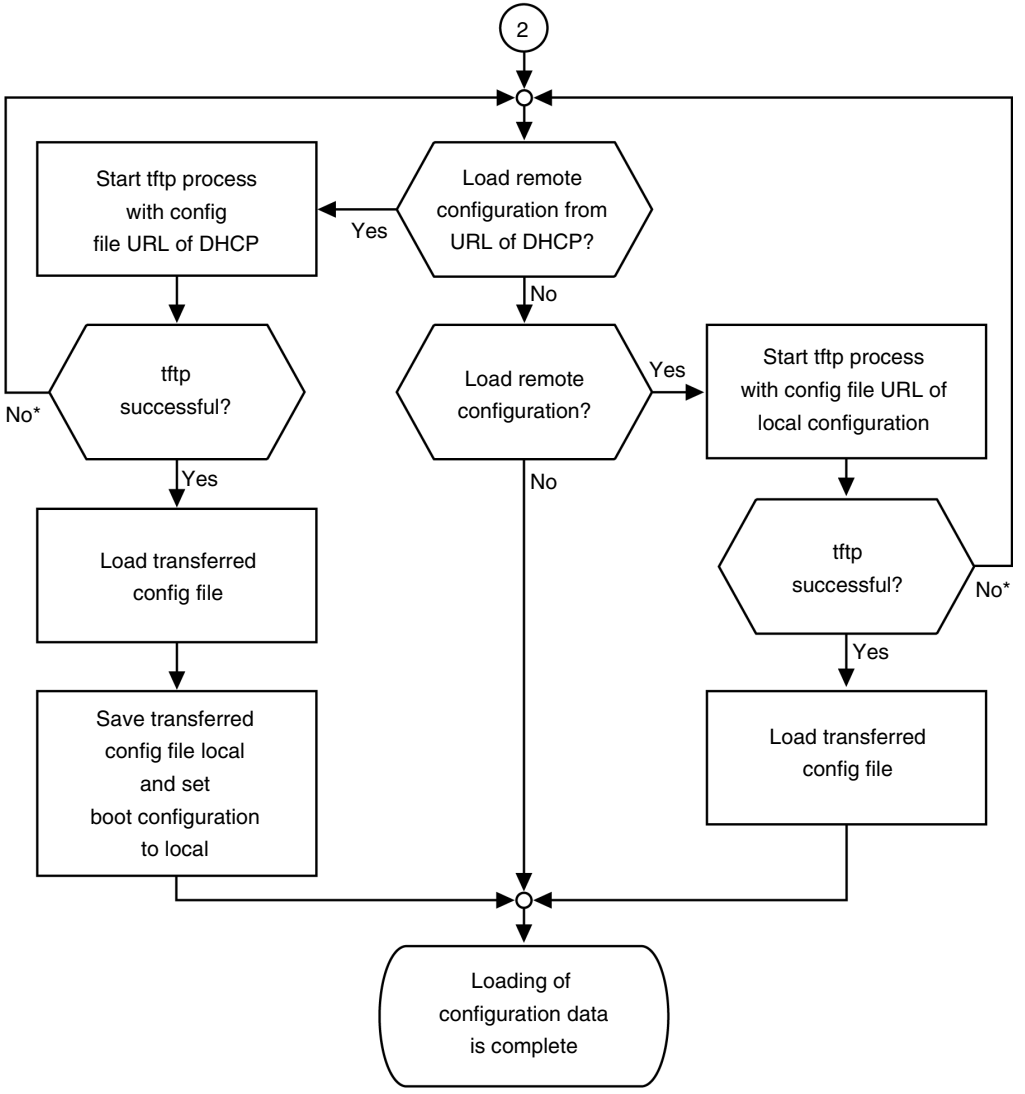
Step	Action
1	Connect the ESM to a serial cable when using the CLI and to an Ethernet cable when using the Web-based interface.
2	Activate DHCP to receive the configuration data in the CLI, or refer to *p. 41*.
3	Change to the privileged EXEC mode by typing `enable`, and press the ENTER key.
4	Enable DHCP by typing `configure protocol DHCP`, and press the ENTER key.
5	Perform the configuration, providing the DHCP server with the required switch data.
6	Save the configuration performed by typing the command `copy system:running nvram:startup-config`, and press the ENTER key.
7	Confirm that you wish to save the configuration by pressing Y.

Flow Chart for the DHCP Process

On startup, an ESM receives its configuration data according to the BOOTP/DHCP procedure described in the following chart:



The following shows part 2 of the BOOTP/DHCP process.



The ESM sends its system name to the DHCP server. The DHCP server can then assign an IP address as an alternative to the MAC address by using the system name.

In addition to the IP address, the DHCP server sends

- the tftp server name (if present) and
- the name of the configuration file (if present).

The ESM accepts this data as configuration parameters (see *p. 41*). If an IP address has been assigned by a DHCP server, it will be permanently saved in the local memory.

The ESM requests these DHCP options:

Option	Meaning
1	subnet mask
2	time offset
3	router
4	time server
12	host name
66	tftp server name
67	bootfile name

The special feature of DHCP in contrast to BOOTP is that the server can only provide the configuration parameters for a certain period of time (lease). When the time period expires (lease duration), the DHCP client must attempt to renew the lease or negotiate a new one. A BOOTP-similar response can be set on the server (i.e., the same IP address is always assigned to a particular client using the MAC address), but this requires the explicit configuration of a DHCP server in the network. If this configuration was not performed, a random IP address (whichever one happens to be available) is assigned.

Default setting is DHCP enabled.

As long as DHCP is activated, the ESM attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.

To activate or deactivate DHCP, refer to *p. 41*.

Below you can view an example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 149.218.112.0 netmask 255.255.240.0 {
    option subnet-mask 255.255.240.0;
    option routers 149.218.112.96;}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
    hardware ethernet 00:80:63:08:65:42;
    fixed-address 149.218.112,82;
    }
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#   option dhcp-client-identifier "hugo";
    option dhcp-client-identifier 00:68:75:67:6f;
    fixed-address 149.218.112.83;
    server-name "149.218.112.11";
    filename "/agent/config.dat";
}
```

Lines that start with a # character are comment lines.The lines preceding the individually listed devices refer to settings that apply to all the following devices.The fixed-address line assigns a permanent IP address to the device.

System Configuration Using DHCP Option 82

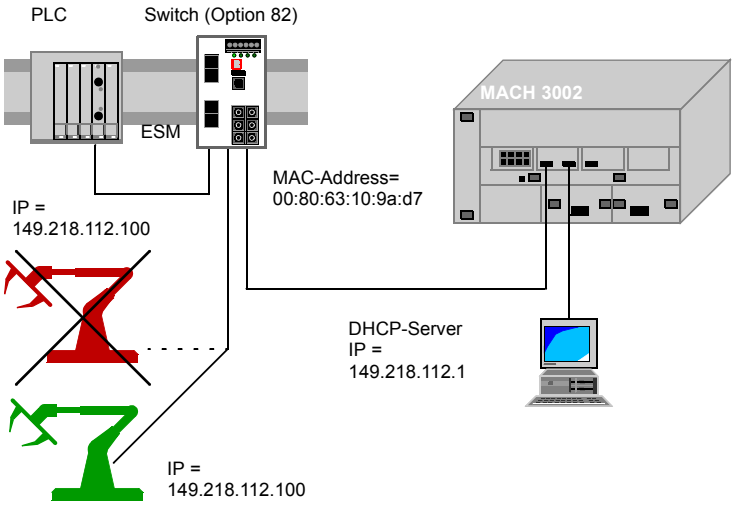
General Information

If you want to configure the system using DHCP Option 82, you need a DHCP server with Option 82. The DHCP server matches the configuration data to the ESM based on its physical connection.

As with the classic DHCP, on startup an agent receives its configuration data according to the BOOTP/DHCP process flow chart (see *p. 36*).

The system configuration is based on the classic DHCP protocol on the device being configured, whereas Option 82 is based on the network topology. This procedure allows you to always assign the same IP address to any device connected to a particular location (port of a switch) on the LAN. For the installation and configuration of a DHCP Option 82 server, refer to *p. 184*.

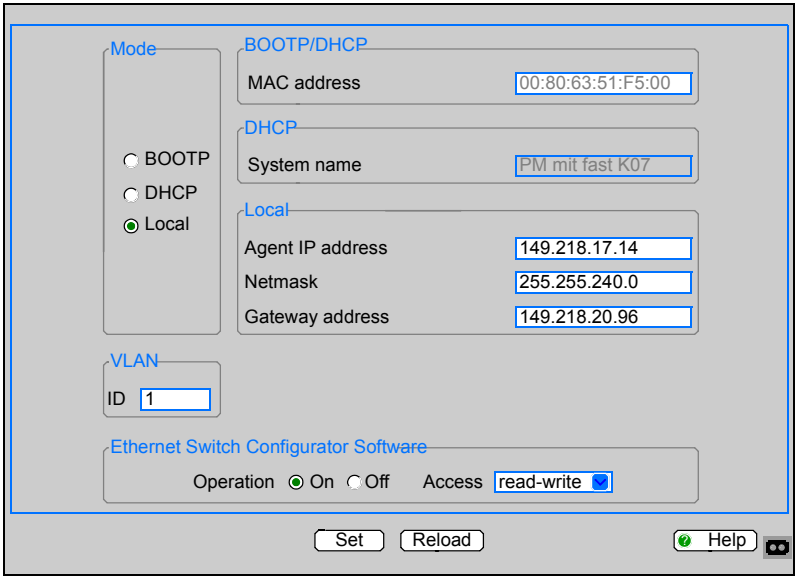
The figure shows an application example of DHCP Option 82.



System Configuration Using the Web-Based Interface

Configuration Procedure Using the Web-Based Interface

Perform the configuration as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Network**. The figure below shows the **Network** dialog box. 
4	Under **Mode**, select where the ESM receives its IP parameters from: ● In the **BOOTP** mode, the configuration parameters are assigned via a BOOTP or DHCP server on the basis of the MAC address of the ESM. ● In the **DHCP** mode, the configuration parameters are assigned via a DHCP server on the basis of the MAC address or the name of the ESM. ● In the **Local** Mode, the net parameters in the ESM memory are used.
5	Enter the parameters according to the mode selected.
6	In the **System Name** line, enter the system name applicable to the DHCP protocol.
7	In the **Local** frame, assign an **Agent IP address**, a **Netmask** and a **Gateway Address** to the ESM.
8	In the **VLAN ID** group box, you can assign a VLAN (see *p. 193*) to the ESM.
9	An alternative method to assign the IP address is to use the Ethernet Switch Configurator software provided with the ESM (see *p. 28*).
10	Save the settings you have made to ensure they are still available after restart (see *p. 50*).

Faulty Device Replacement

Solutions for Faulty Device Replacement

There are two plug-and-play solutions available for replacing a faulty ESM:

- First, you can configure the new switch using an Memory back up adapter (EAM) (see *p. 46*).
- Second, you can configure the new switch using DHCP Option 82 (see *p. 40*).

In both cases, the same configuration data which the faulty ESM had are transferred to the new ESM during booting.

Loading and Saving Settings

3

At a Glance

Overview

This chapter provides information concerning the loading and saving procedures for the settings you have made.

What's in this Chapter?

This chapter contains the following topics:

Loading Settings

Sources for Loading Settings

During operation, the ESM enables you to load settings from the following sources:

- the local non-volatile memory
- the Memory back up adapter (If a Memory back up adapter (EAM) is connected to the ESM, the ESM always loads its configuration from the EAM.)
- a file on the connected network (= default setting)
- default settings

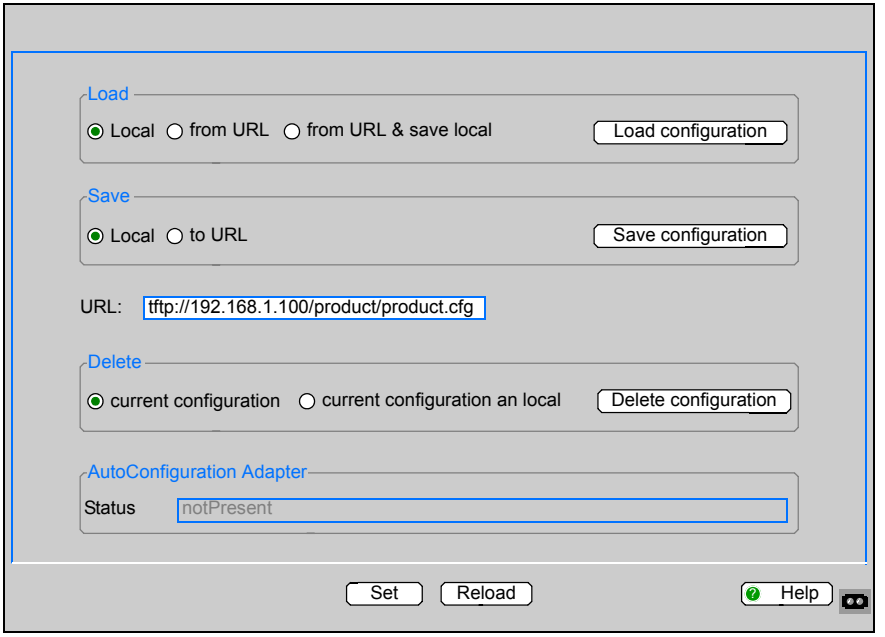
Note: When loading a configuration, do not access the switch until it has loaded the configuration file and has made the new configuration settings.
Depending on the complexity of the configuration settings, this procedure can last between 10-200 seconds.

Loading from the Local Non-Volatile Memory

Note: During restart, the switch automatically loads its configuration data from the local non-volatile memory, provided that you have not activated BOOTP/DHCP and that no EAM (see EAM) is connected to the switch.

Loading Settings from the Local Non-Volatile Memory Using the Web-Based Interface

Proceed as follows in the Web-Based Interface:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Load/Save**. The figure below shows the **Load/Save** dialog box. 
4	Click **Local** in the group box **Load**.
5	Click **Load Configuration**.

Loading Settings from the Local Non-Volatile Memory Using the Command Line Interface (CLI)

Proceed as follows in the CLI:

Step	Action
1	Connect the ESM to a serial cable.
2	Open the CLI.
3	Enter the command `enable` to change to the privileged EXEC mode.
4	Enter the command `copy nvram:startup-config system:running-config` to load the configuration data from the local non-volatile memory.

Loading Settings from the Memory back up adapter (EAM)

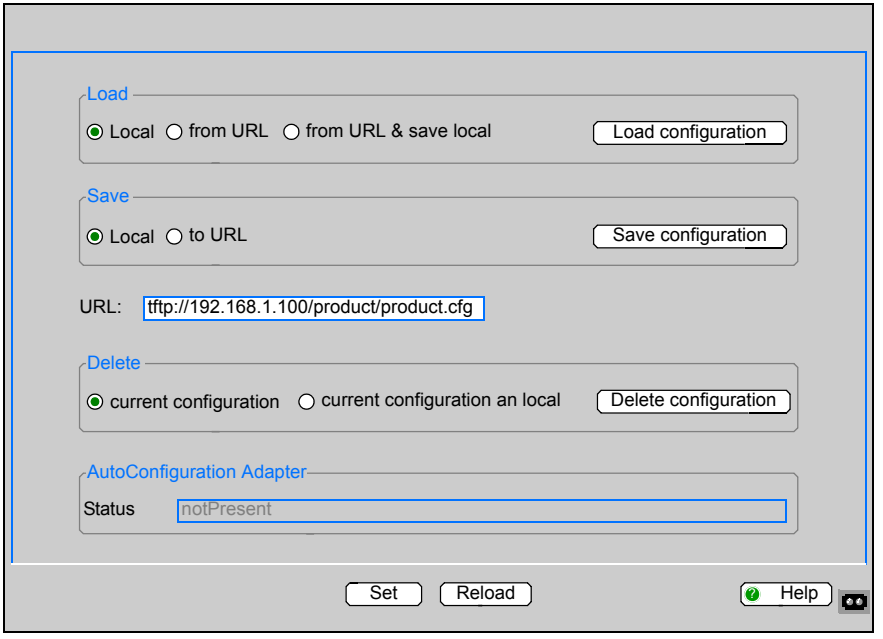
If an EAM is connected to the ESM, the ESM always loads its configuration from the EAM. For information on how to save a configuration file onto an EAM, refer to *p. 50*.

Loading Settings from a File

The ESM enables you to load the configuration data from a file in the connected network, provided that no EAM is connected to it.

Loading Settings from a File Using the Web-Based Interface

Load the settings as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Load/Save**. The figure below shows the **Load/Save** dialog box. 
4	Click **from URL** in the group box **Load** if you want the ESM to load the configuration data from a file and to retain the locally saved configuration. Click **from URL & Save Locally** in the group box **Load** if you want the ESM to load the configuration data from a file and to save this configuration locally.
5	In the **URL** edit box, type the field path under which the ESM finds the configuration file.
6	Click **Load Configuration**.

Example of Loading a File from the TFTP Server Using the Web-Based Interface

Load a file from the tftp server as follows:

Step	Action
1	To enable yourself to download a file from the tftp server, save the configuration file into the corresponding path of the tftp server with the file name, e.g. *switch/switch_o1.cfg* (see *p. 51*).
2	Type the path to the tftp server in the edit box **URL**, e.g. *tftp://149.218.112.5/ESM/config.dat*. To load from an ETY or NOE module, the URL is: `tftp://IPaddress//RAM0/switch rolename.prm` where the *IPaddress* is the IP address of the module and *switch rolename* is the roll name assigned to the switch.

Trouble Shooting Using the Web-Based Interface

You can trouble shoot as follows:

Step	Action	Comment
1	View the status of the loading procedure in the selected option **URL & Save Locally** of the group box **Load**.	If you get an error message while saving the configuration, one reason may be that the loading procedure has not been completed. DHCP/BOOTP does not finish the loading procedure until a valid configuration has been loaded.
2	If DHCP/BOOTP cannot find any valid configuration, stop the active loading procedure by loading the local configuration via the **Load** group box.	

Loading Settings from a File Using the CLI

Load settings from a file as follows:

Step	Action
1	Connect the ESM to a serial cable.
2	Open the CLI.
3	Enter the `enable` command to change to the privileged EXEC mode.
4	Enter the command `copy tftp://149.218.112.159/switch/config.dat nv-ram:startup-config` if you want the switch to load the configuration data from a tftp server in the connected network.

Resetting the Configuration to the Default Settings

The switch enables you to

- reset the current configuration to the default settings (The locally saved configuration is retained.),
- reset the ESM to the default settings. After a restart, the IP address is also set to the default setting.

Resetting the Configuration to the Default Settings Using the Web-Based Interface

Reset the configuration to the default settings as follows:.

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Load/Save**.
4	In the group box **Delete**, click either **current configuration** or **current configuration and local**.
5	Click **Delete configuration**.

Resetting the Configuration to the Default Settings Using the System Monitor

Reset the configuration to the default settings as follows:

Step	Action	Comment
1	Connect the ESM V.24 socket to a terminal or VT 100 emulator PC using a terminal cable.	
2	Open the System Monitor.	
3	Select **5 Erase main configuration file**.	This menu allows you to reset the switch to its default settings. The ESM saves configurations which differ from the default settings in the *ESM.cfg* file of the flash memory.
4	Press the ENTER key to delete the *ESM.cfg* file.	

Saving Settings

Options for Saving Settings

The ESM enables you to save the settings you have made

- locally,
- locally and on the EAM, or
- to a file.

Saving Locally and on the EAM Using the Web-Based Interface

Save the current configuration data as follows:.

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Load/Save**.
4	Click **Local** in the **Save** group box.
5	Click **Save Configuration**. As a result, the ESM saves the current configuration data to the local non-volatile memory and, provided that an EAM is connected, also to the EAM.

Saving Locally and on the EAM Using the CLI

Save the current configuration data as follows:

Step	Action
1	Connect the ESM to a serial cable.
2	Open the CLI.
3	Enter the command `enable` to change to the Privileged EXEC mode.
4	Enter the command `copy system:running-config nvram:startup-config` to save the current configuration data to both the local non-volatile memory and to the EAM if an EAM is connected.

Saving to a File Using the Web-Based Interface

Save the configuration data to a file as follows:.

Step	Action	Comment
1	Connect the ESM to an Ethernet cable.	
2	Open the Web-based interface.	
3	Go to **Basics** → **Load/Save**.	
4	Click **to URL** in the **Save** group box.	
5	Type in the **URL** edit field the path under which you want the ESM to save the configuration file.	
6	Click **Save Configuration**.	The URL marks the path to the tftp server on which the switch saves the configuration file. The URL is written as follows: *tftp://IP address of the tftp server/path name/file name*, e.g. *tftp://149.218.112.5/switch/config.dat*. To save from an ETY or NOE module, the URL is: `tftp://IPaddress//RAM0/switch rolename.prm` where the *IPaddress* is the IP address of the module and *switch rolename* is the roll name assigned to the switch.

Configuration Data

Note: The configuration file contains all configuration data, including the password. Thus, note the access rights on the tftp server.

Saving to a File Using the CLI

This table outlines the procedure to save the current configuration data to a file using the command line interface.

Step	Action
1	Connect the ESM to a serial cable.
2	Open the CLI.
3	Enter the command `enable` to change to the privileged EXEC mode.
4	Enter the command `copy nvram:startup-config tftp://149.218.112.159/switch/config.dat` if you want the switch to load the current configuration data from a tftp server in the connected network.

Loading Software Updates

4

At a Glance

Overview

This chapter explains how to update your ESM software.

What's in this Chapter?

This chapter contains the following topics:

Loading Software from the EAM Memory Back-up Adapter

Checking the Software Release Installed Using the Web-Based Interface

Check the software release installed on your ESM as follows:

Step	Action
1	Open the Web-based interface.
2	Connect the ESM with an Ethernet cable.
3	Go to **Basics** → **Software** to view the release number of the software installed on your ESM.

Loading Procedure Using the CLI

Load the software from the EAM as follows:

Step	Action	Comment
1	Connect the EAM to which you have copied the ESM software to the USB port of the ESM.	
2	Connect the ESM to a terminal or a VT 100 emulator using a terminal cable.	
3	Start the terminal program on the PC and establish a connection with the ESM.	
4	Reboot the ESM.	While the ESM is booting, the following message appears on the terminal: `Press <1> to enter System Monitor 1...`
5	Type `1` within 1 s to start System Monitor 1.	System Monitor 1 displays the following: **1.** `Select Boot Operating System` **2.** `Update Operating System` **3.** `Start Selected Operating System` **4.** `End (reset and reboot)` **5.** `Erase main configuration file` **6.** `Show Bootcode Information`
6	Select **2**, and press the ENTER key to copy the software from the EAM into the local memory of the ESM.	On concluding the update, the System Monitor prompts you to press any key to continue.
7	Select **3** to start the new software on the ESM.	

Loading the Software from the EAM Using a Computer

Like a standard USB memory stick, you can also connect the EAM to an USB port of your PC and copy the ESM software to the main directory of the EAM (see *p. 50*).

Further System Monitor Options

In addition, the System Monitor features further options in connection with your ESM software:

- swapping the software images available
- performing a cold start

Swapping the Software Images

Swap the software images as follows:

Step	Action	Comment
1	On the start screen of the System Monitor, select **1 Boot Operating System**..	A new screen appears.
2	On the new screen, select **1** to swap the two software images available (In connection with the swapping of the images see also **1 - 7**).	**1 Swap Os images** The memory of the ESM offers space for two images of the software. Via this item you can load a new version of the software without erasing the existing version. **2 Copy image to backup** Via this item you can save a copy of the active software. **3 Test stored images in Flash mem.** Via this item you can test whether the stored images in the flash memory contain valid codes. **4 Test stored images in USB mem.** Via this item you can test whether the stored images of the software on the EAM contain valid codes. **5 Apply and store selection** Via this item you can apply and store the selection of the software. **6 Reformat Flash file system** Via this item you can reformat the flash file system. **7 Cancel selection** Via this item you can cancel the selection and leave this dialog without changes.

Performing a Cold Start

Perform a cold start as follows:

Step	Action
1	On the start screen of the System Monitor, select **4 End (reset and reboot)** to perform a cold start.

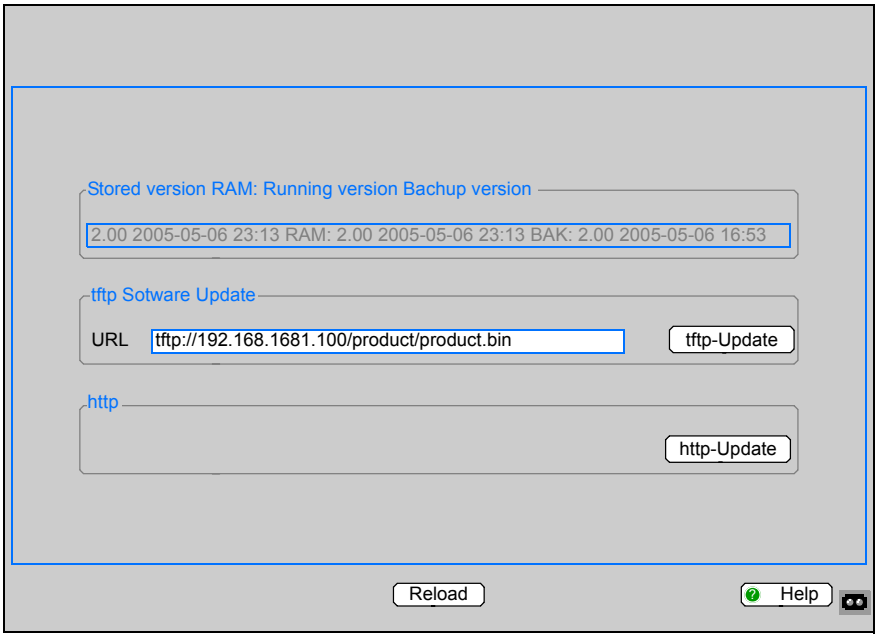
Loading Software Updates from the TFTP Server

TFTP Server

Note: For a tftp (see tftp) update you need a tftp server on which the ESM software you wish to load is saved.

Loading Procedure Using the Web-Based Interface

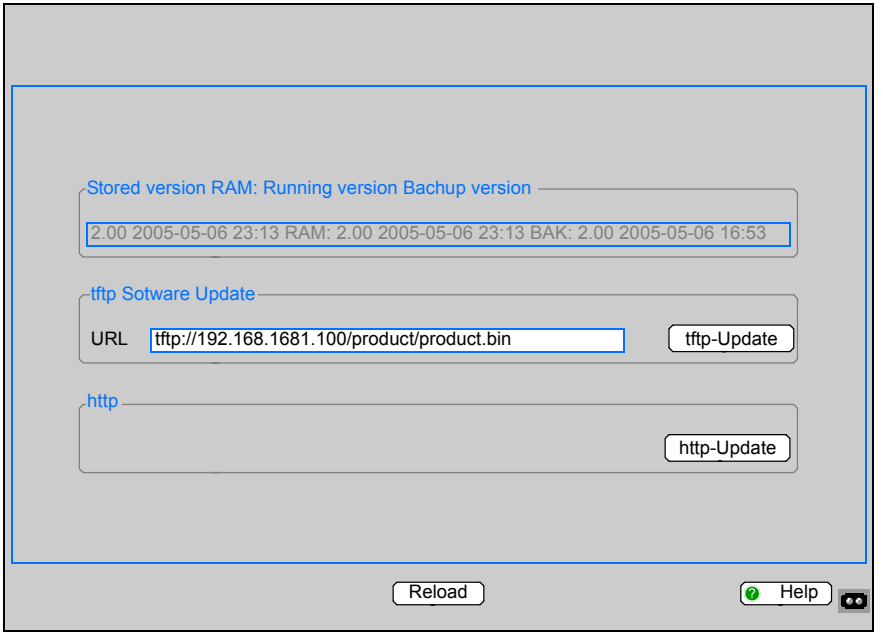
Download ESM software updates from the tftp server as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Software**. The screen below shows the **Software** dialog box.  The URL identifies the path to the software stored on the tftp server. It is written as follows: *tftp://IP address of the tftp server/path name/file name (e.g. tftp://149.218.112.4/esm/esm.bin*.
4	Click **tftp Update** to load the software from the tftp server onto the switch.
5	After the loading procedure has been completed successfully, activate the new software as follows: Go to **Basics** → **Restart**, and perform a cold start.
6	After booting the switch, click reload in your browser to re-enable your access to the ESM.

Loading Software Updates via HTTP

Loading Procedure

Proceed as follows to update the software on your switch:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Software**. The following dialog box appears: 
4	Click **http Update** to open the **http Update** browser window.
5	Click **Browse** to select the software on you PC for the update.
6	Click **Update** to transfer the software to the switch. One of the following messages is displayed when the update has been completed: ● Update completed successfully. ● Update failed. Reason: incorrect file. ● Update failed. Reason: file damaged. ● Update failed. Reason: flash error.
7	Close this browser window: **File** → **Close** to return to the **Software** dialog box.
8	After the software procedure has been completed successfully, go to **Basics** → **Restart**, and perform a cold start by clicking **Restart Swtich**.
9	Click **Reload** in your browser to re-enable ESM access after booting.

Port Configuration

5

At a Glance

Overview

This chapter provides information concerning the port configuration procedure.

What's in this Chapter?

This chapter contains the following topics:

Switching the Ports On and Off

Enhancing Access Security

In the the default setting is all ports are switched on. To enhance access security, switch off the ports which you do not wish to connect.

Procedure Using the Web-Based Interface

Switch the ports on and off as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Port Configuration**.
4	Select in the column **Port On** the ports which a device will be connected to.

Selecting the Operation Mode

Default Settings

The default setting for all ports is **Auto-negotiation** mode.

Procedure Using the Web-Based Interface

Change to **Auto-negotiation** mode as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Port Configuration**.
4	If the device connected to this port requires a fixed setting ● select the operation mode (transfer speed, duplex operation) in the **Manual Configuration** column, ● and deactivate the port in the **Auto-negotiation** column.

Note: The active auto-negotiation has priority over the manual configuration.

Displaying Connection Error Messages

General Information

If the ESM is set to default, it will display a connection error via the signal contact and the LED display. The ESM allows you to disable the displaying of connection error messages, for instance to prevent a device that has been turned off from being interpreted as an interrupted line.

Activating Connection Error Messages

Activate the connection error messages as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Port Configuration**.
4	In the **Signal Contact mask** column, select the ports whose connections you want to mask the displaying of the connection error message.

Protection from Unauthorized Access

6

At a Glance

Overview

This chapter provides information on how to protect your network from unauthorized access.

What's in this Chapter?

This chapter contains the following topics:

The Password for SNMP Access

Description of the Password for SNMP

A network management station communicates with the switch via the Simple Network Management Protocol (SNMP).

Every SNMP packet contains the IP address of the sending computer and the password under which the sender of the packet would like to access the switch MIB.

The switch receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the MIB of the switch. If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the switch will allow access.

The default setting is that the switch can be accessed using the **public** (read only) and the **private** (read and write) passwords and their respective login names (**user** or **path**) from every computer.

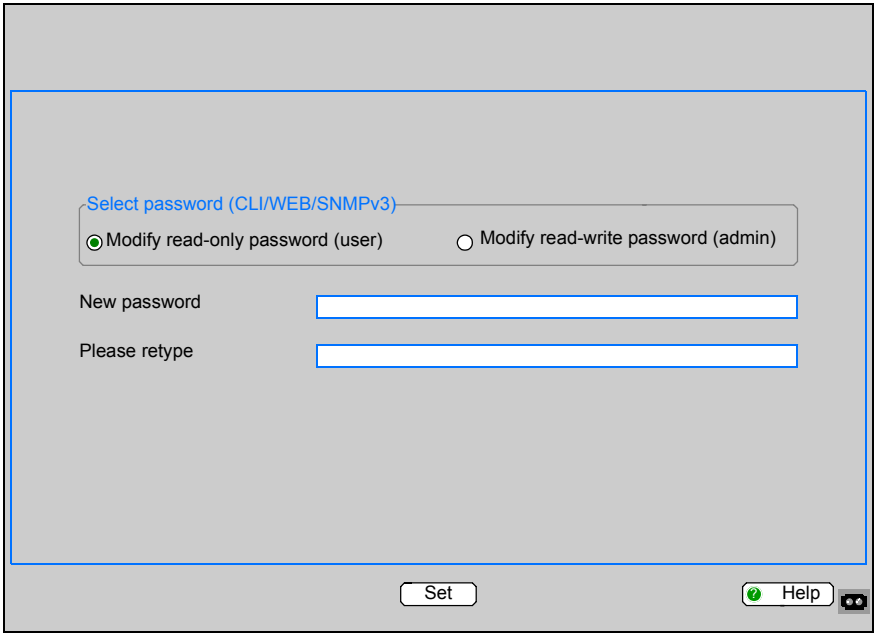
Protecting your Switch from Unwanted Access

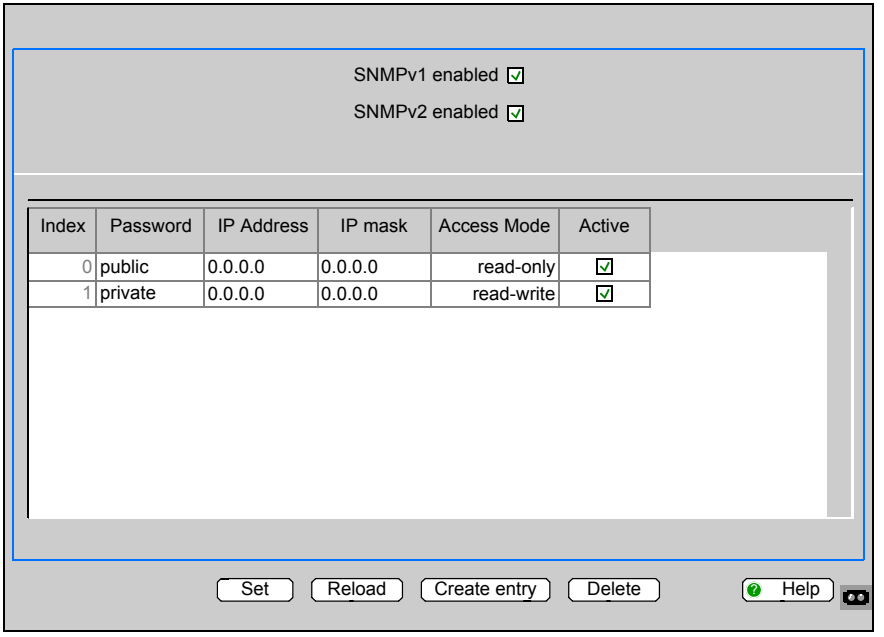
Protect your switch from unauthorized access as follows:

Step	Action
1	Define a new password which you can access from your computer with all rights.
2	Treat this password with discretion, as everyone who knows the password can access the switch MIB with the IP address of your computer.
3	Limit the access rights of the known passwords, or delete their entries.

Entering the Password for SNMP Access Using the Web-Based Interface

Proceed as follows to enter the password for SNMP access:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Security** → **Password/SNMP**. The dialog enables you to change the read and read/write passwords for access to the ESM via the Web-based interface/CLI/SNMP. Please note that passwords are case-sensitive. For security reasons, the read password and the read/write password must not be identical. The Web-based interface and the user interface communicate using SNMP version 3. The following figure is displayed on the screen: 
4	Select **Modify read-only password (user)** to enter the read-only password.
5	Enter the new read-only password in the line **New password**, and repeat the entry in the line **Please retype**.
6	Select **Modify read-write password (admin)** to enter the read-write password.

Step	Action
7	Enter the new read-write password in the line **New password**, and repeat the entry in the line **Please retype**. **Note:** If you do not know a password with read/write access, you will not have access to the ESM! **Note:** After changing the password for write access, restart the Web-based interface to access the ESM. **Note:** For security reasons, the passwords are not displayed. Note down each change! You cannot access the ESM without a valid password! **Note:** For security reasons, SNMP version 3 encrypts the password. Enabling SNMPv1 or SNMPv2 unencrypts the password. **Note:** As many applications do not accept passwords shorter than 8 characters, you should use 8characters for the password.
8	To unencrypt the password, go to **Security** → **SNMPv1/v2 Access**, and select **SNMPv1 enabled** or **SNMPv2 enabled**. As many applications do not accept passwords shorter than 8 characters, you should use 8 characters for the password in SNMP version 3.
9	Go to **Security** → **SNMPv1/v2**. The following dialog box appears.  The **SNMPv1/v2** dialog box allows you to select the access using SNMPv1 or SNMPv2. The default setting for SNMPv1/v2 is both protocols are enabled, which allows you to communicate with earlier versions of SNMP. Please note that passwords are case-sensitive.

Step	Action
10	To be able to communicate with earlier versions of SNMP, select **SNMPv1/2 enabled**.
11	Select **SNMPv1 enabled** or **SNMPv2 enabled** in the table to determine which IP addresses are allowed to access the ESM and which type of passwords are to be used. The table allows you to create up to 8 entries. For security reasons, the read password and the read/write password must not be identical. Please note that passwords are case-sensitive.
12	To create a new line in the table **Click Create entry**.
13	To delete an entry, select the line in the table and click **Delete**. The items in the table have the following meanings: ● **Index**: current number for this table entry ● **Password**: password the computer must use to have access to the ESM; This password is independent of the SNMPv3 password. ● **IP address** IP address of the computer permitted to access the ESM ● **IP mask** IP mask to the IP address ● **Access Mode** determines if the computer has read-only or write access ● **Active** enabling/disabling this entry

Setting the Telnet/Web-Based Access

Description of Telnet Access

The Telnet server of the ESM allows you to configure the ESM using the Command Line Interface (CLI). You can switch off the Telnet server to prevent Telnet access to the ESM.

The default setting is that the server is switched on.

After the Telnet server has been switched off, the ESM can no longer be accessed using a Telnet connection.

Note: The Telnet server may be reactivated using the CLI or the Web-based interface via **Security** → **Telnet/Web Access**.

Description of Web-Based Access

The Web server of the ESM allows you to configure the ESM using the Web-based interface. You can switch off the Web server to prevent Web access to the ESM.

The default setting is that the server is switched on.

After the Web server has been switched off, the ESM can no longer be accessed using a Web browser.

Note: The Web server may be reactivated using the CLI.

Disabling and Enabling Telnet or Web-Based Access Using the Web-Based Interface

You can disable and enable Telnet or Web access as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-Based interface.
3	Go to **Security** → **Telnet/Web Access**.
4	Switch off/on the server to which you wish to disable/enable access.

Enabling and Disabling Telnet Access Using the Command Line Interface (CLI)

You can enable and disable Telnet access as follows:

Step	Action
1	Connect the ESM to a serial cable.
2	Open the CLI.
3	Enter the command `enable` to change to the privileged EXEC mode.
4	Enter the command `transport input telnet` to switch on the Telnet server.
5	Enter the command `no transport input telnet` to switch off the Telnet server.

Enabling and Disabling Web-Based Access Using the CLI

You can enable and disable the Web access via the CLI as follows:

Step	Action
1	Enter the command `enable` to switch to the privileged EXEC mode.
2	Enter the command `ip http server` to switch on the Web server.
3	Enter the command `no ip http server` to switch off the Web server.

Disabling the Ethernet Switch Configurator (ESC) Function

Description of the ESC Software

The ESC software (see *p. 28*) allows you to assign an IP address to the ESM on the basis of its MAC address.

Note: For security reasons, either limit or switch off completely the ESC function of the ESM after assigning the IP parameters.

Disabling and Limiting the ESC Function Using the Web-Based Interface

You can disable or limit the ESC function as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Network**.
4	Switch off the ESC function in the **Ethernet Switch Configurator Software** group box, or limit access to **Read Only**.

Disabling, Limiting and Enabling the Ethernet Switch Configurator Function Using the Command Line Interface

You can disable, limit or enable the Ethernet Switch Configurator function as follows:

Step	Action
1	Connect the ESM to a serial cable.
2	Open the CLI.
3	Type the command `enable` to switch to the privileged EXEC mode.
4	Type the command `network protocol Ethernet Switch Configurator off` to switch off the Ethernet Switch Configurator function.
5	Type the command `network protocol Ethernet Switch Configurator read-only` to switch on the ESC function with the **Read** access right.
6	Type the command `network protocol Ethernet Switch Configurator read-write` to switch on the ESC function with the **Read and Write** access right.

Port Access Control

Description of Port Access Control

The ESM protects every port from unauthorized access.

Depending on your choice, the ESM checks either the MAC address or the IP address of the connected device.

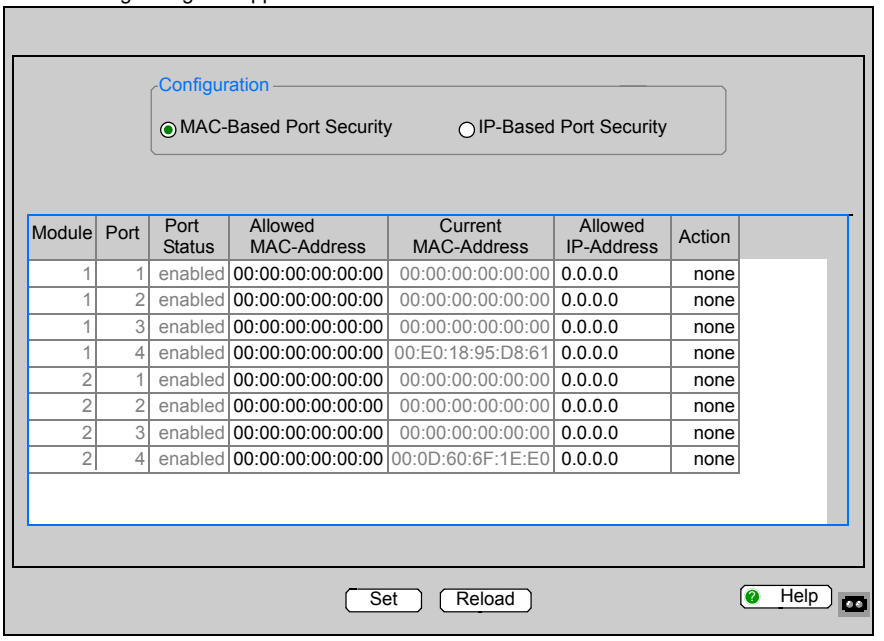
The following functions are available for monitoring every individual port:

- Who has access to this port?
  The ESM recognizes two classes of access control:
  - all: There is no access restriction.
  - user: Only an assigned user has access.
    You define this user with his MAC or IP address.
- What should happen after an unauthorized access attempt?
  The ESM can respond in three selectable ways to an unauthorized access attempt:
  - none: no response
  - trapOnly: message by sending a trap
  - portDisabled: message by sending a trap and disabling a port

Note: Since the ESM is a layer 2 device, it translates the stored IP addresses into MAC addresses. In so doing, a MAC address should be assigned to exactly one IP address. Please bear in mind that when you use a router, several IP addresses can be assigned to one MAC address, namely that of the router. This means that all packets of the router will pass the port unchecked if the permitted IP address is that of the router. If a connected device sends packets with other MAC addresses and a permitted IP address, the ESM will disable the port.

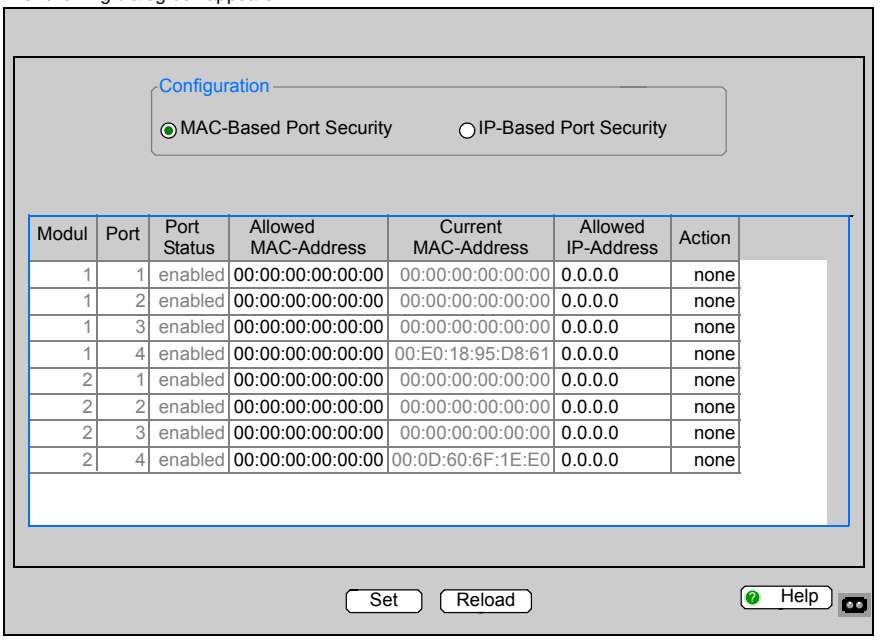
Defining IP-Based Port Access Control Using the Web-Based Interface

Define IP-based port access control as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Security** → **Port Security**. The following dialog box appears. 
4	Choose **IP-Based Port Security**.
5	Enter in the **Allowed IP address** column the IP address of the device with which data exchange is permitted at this port. Without an entry, data can be received from any device.
6	In the **Action** column, select one of the following reactions to an unauthorized access attempt: ● no action (**none**) ● message by sending a trap (**trapOnly**) ● the respective port in the **Port Configuration** table is disabled (see *p. 59*) and trap (**portDisabled**) is sent. An entry in the **Port Configuration** table is part of the configuration and is saved with the configuration. An alarm (trap) can only be sent if at least one recipient is entered under *Configuring Traps Using the Web-Based Interface, p. 112* and if both the appropriate status and **Port Security** are marked.

Defining MAC-Based Port Access Control Using the Web-Based Interface

Define the MAC-based port access control as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-Based Interface.
3	Go to **Security** → **Port Security**. The following dialog box appears. 
4	Choose **MAC-Based Port Security**.
5	In the **Allowed MAC Address** column, enter the MAC address of the device with which data exchange is permitted at this port. Without an entry, data can be received from any device.
6	Press the left mouse button to copy an entry from the **Current MAC Address** column into the **Allowed MAC Address** column. The **Current MAC Address** column shows the MAC address of the device from which data was received last.
7	In the **Action** column, select one of the following reactions to an unauthorized access attempt: ● no action (**none**) ● message by sending a trap (**trapOnly**) ● the respective port in the **Port Configuration** table is disabled (see *p. 59*) and trap (**portDisabled**) is sent. An entry in the **Port Configuration** table is part of the configuration and is saved with the configuration. An alarm (trap) can only be sent if at least one recipient is entered under *Configuring Traps Using the Web-Based Interface, p. 112* and if both the appropriate status and **Port Security** are marked.

Synchronizing the System Time of the Network

7

At a Glance

Overview

This chapter contains information concerning the synchronization of the system time of the network.

What's in this Chapter?

This chapter contains the following topics:

Protocols for Synchronizing the System Time of the Network

SNTP and PTP

When you synchronize the system time of the network, the ESM allows you to use either the Simple Network Time Protocol (SNTP) or the Precision Time Protocol (PTP). The accuracies of both protocols differ.

If you only require accuracies in the order of milliseconds, the Simple Network Time Protocol (SNTP) offers a low-cost solution.

Areas of application of this protocol are:

- log entries
- time stamping of production data
- production control

The Precision Time Protocol (PTP), which is described in the IEEE 1588 standard, achieves accuracies in the order of fractions of microseconds.

Note: Choose the protocol which best meets your requirements. When using both protocols at the same time, bear in mind that they interact.

Entering the System Time

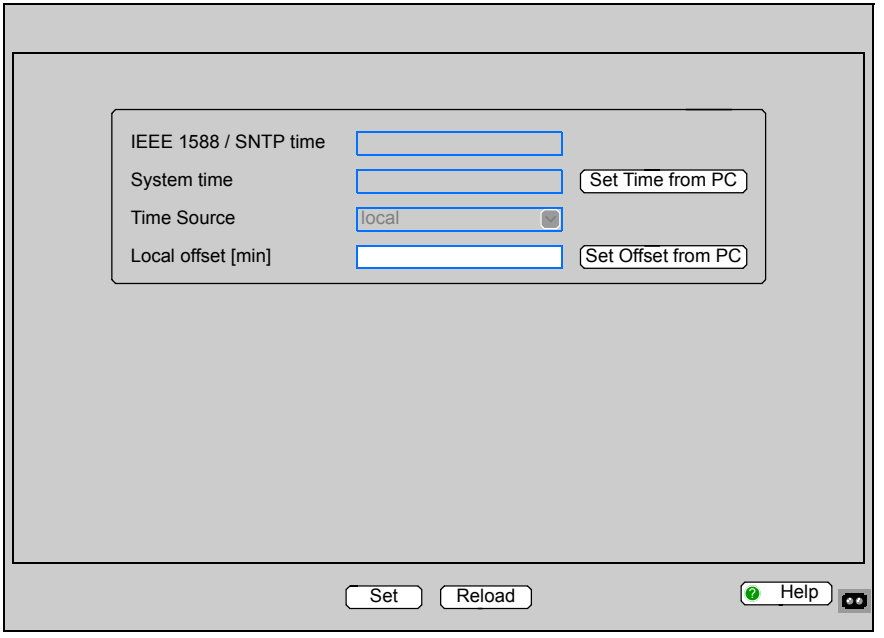
Entering the System Time Using PTP or SNTP

If there is no reference watch available, you can enter the system time in the ESM so that you can use it like a reference clock (see *p. 80*).

Making Time-Related Settings Using the Web-Based Interface

Make settings independent of PTP or SNTP as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Time**.
4	Make your time-related settings in the screen below.



Possible Time-Related Settings

You can make the following settings independent of PTP or SNTP:

- IEEE 1588 Time displays the time received via PTP. **SNTP Time** displays the time with reference to Universal Time Coordinated (UTC). This means the same time is displayed worldwide and that differences are not taken into account.
- System Time uses **IEEE 1588/SNTP time**, allowing for the local time difference of **IEEE 1588/SNTP time**:
  System Time = **IEEE 1588/SNTP time** + **Local offset**.
- Time Source displays the origin of the following time. The ESM automatically selects the source with the highest precision.
- If you click **Set Time from PC**, the switch will load the PC's time as the system time and calculate **IEEE 1588/SNTP time**, allowing for the local time difference. **IEEE 1588/SNTP time** = **System time** - **Local offset**.
- Local offset allows you to display/enter the time difference between local time and **IEEE 1588/SNTP time**.
- If you click **Offset from PC**, the switch will calculate the time zone on your PC, on the basis of which it will calculate the local time difference.

Note: When setting the time zones with summer and winter times, make an adjustment for the local offset. The switch can also receive the IP address of the SNTP server as well as the local offset from a DHCP server.

Setting the System Time and Entering Differences Between IEEE 1588 and SNTP Time Using the CLI

Set the system time and enter the difference between SNTP and IEEE 1588 as follows:

Step	Action
1	Connect the ESM to a serial cable.
2	Open the CLI.
3	Enter the command `enable` to change to the privileged EXEC mode.
4	Enter the command `configure` to change to the configuration mode.
5	Enter the command `sntp time <YYYY-MM-DD HH:MM:SS>` to set the switch system time.
6	Enter the command `sntp client offset <-1000 to 1000>` to enter the time offset between local time and IEEE1588/SNTP Time.

Simple Network Time Protocol (SNTP)

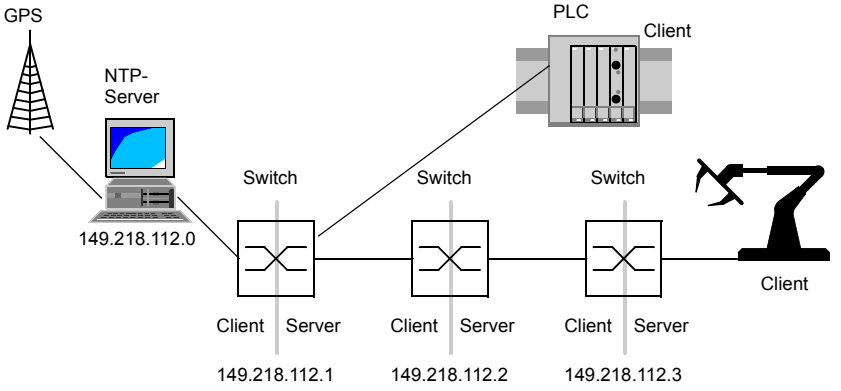
Description of SNTP

SNTP has a hierarchical structure. The SNTP server provides Universal Time Coordinated (UTC). UTC is the time which is referenced to SNTP. The same time is displayed worldwide.

Local time differences are not taken into account.

The ESM supports the SNTP server and the SNTP client functions.

The figure below shows a SNTP application example.



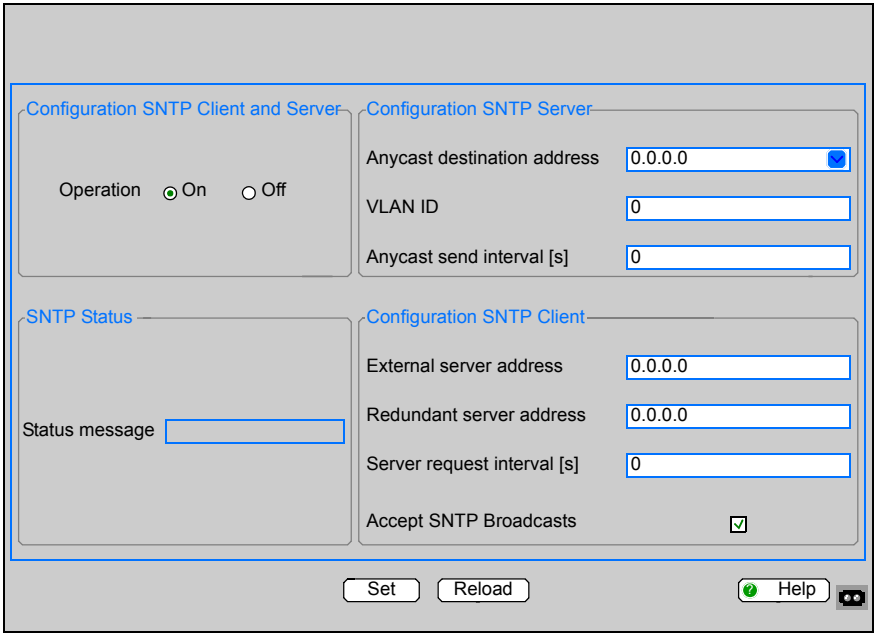
Preparing the SNTP Configuration

Prepare the configuration as follows:

Step	Action
1	To gain an overview of how the system time is passed on, draw a network plan which shows all devices involved in SNTP. Please bear in mind that the accuracy of the system time depends on signal running time.
2	Switch on the SNTP function on all devices whose time you want to set using SNTP.
3	If you do not have a reference clock at your disposal, use a switch as the reference clock, and set its system time as accurately as possible.

Note: To ensure the most accurate system time distribution possible, do not use network components (routers, switches) which do not support SNTP in the signal path between the SNTP server and the SNTP client.

Configuring SNTP Configure the SNTP as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Time** → **SNTP**. The figure below shows the **SNTP** dialog. 
4	In the **Configuration SNTP Client and Server** group box, switch the SNTP function on or off. When it is switched off, the SNTP server does not send any SNTP packages and does not reply to any SNTP requests. The SNTP client does not send any SNTP requests and does not interpret any broadcast/multicast packages.
5	Go to the **SNTP Status** group box to view server conditions under **Status message** such as **Server cannot be reached**.
6	Go to the **Configuration SNTP Server** group box, and enter under **Anycast destination address** the IP address to which the SNTP server on the switch sends the SNTP data packets (target address: 224.0.1.1, the SNTP packets are sent to multicast).
7	Go to the **Configuration SNTP Server** group box, and specify under **VLAN ID** the VLAN to which the ESM may periodically send SNTP packets.

Step	Action
8	Go to the **Configuration SNTP Server** group box, and specify under **Anycast send interval** the interval at which the ESM sends SNTP packets (valid entries: 1 second to 3600 seconds, default: 120 seconds).
9	Go to the **Configuration SNTP Client** group box, and enter under **External server address** the IP address of the SNTP server from which the switch periodically obtains the system time.
10	Go to the **Configuration SNTP Client** group box, and enter under **Redundant server address**, enter the IP address of the SNTP server from which the ESM periodically obtains the system time if the ESM does not receive an answer from the **External Server Address** within 0.5 seconds after making the query. **Note:** If you receive the system time from an external/redundant server address, do not accept any SNTP broadcasts. Otherwise you do not know whether the ESM displays the time from the server entered, or the time from an SNTP broadcast package.
11	Go to the **Configuration SNTP Client** group box, and specify under **Server request interval** the interval at which the EMS requests SNTP packages (valid entries: 1 second to 3600 seconds, default 30 seconds).
12	Click **Accept SNTP Broadcasts** if you want the switch to obtain the system time from SNTP broadcast/ multicast packages which it receives.

Configuration Example

The following table shows a configuration example:

Switch	**149.218.112.1**	**149.218.112.2**
Operation	On	On
Anycast Destination Address	224.0.1.1	224.01.1
Server VLAN ID	1	1
Anycast Send Interval	120	120
Client External Server Address	149.218.112.0	149.218.112.1
Server Request Interval	30	30
Accept SNTP Broadcasts	No	No

Precision Time Protocol (PTP)

Function Description of PTP

The requirement for running time-critical applications over a LAN is a precision time management system. The IEEE 1588 standard with the Precision Time Protocol describes a procedure that is based on the reference clock principle. This means that the clocks in a LAN are synchronized according to the most precise clock reference or grandmaster clock) in that LAN.

This procedure permits synchronization of the clocks with an accuracy on the scale of hundredths of nanoseconds. The synchronization messages have virtually no effect on the network load. PTP uses multicast communication.

Factors influencing precision are:

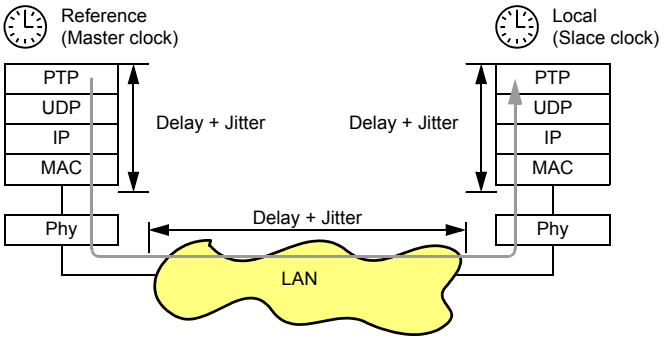
- Accuracy of the Reference Clock IEEE 1588 classifies clocks according to their accuracy. An algorithm that measures the accuracy of the available clocks in the network determines the most accurate time for the grandmaster clock.

The following table explains what some stratum numbers stand for.

Stratum Number	Specification
0	To assign for temporary, special purposes a better value to one clock than to all other clocks within the network.
1	Designates the clock with the highest precision as the reference clock. A stratum 1 clock can be both a boundary and an ordinary clock. Stratum 1 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock cannot be synchronized using PTP from another clock in the PTP system.
2	Designates the clock as the second-choice reference clock and cannot be synchronized using PTP from another clock in the PTP system.
3	Designates the clock that can synchronize other devices using an external cable as the reference clock.
4	Designates the clock as the reference clock.
5-254	Reserved
255	Default Setting (Such a clock should never be the best master clock).

- Cable Delays; Device Delays
  The communication protocol defined by IEEE 1588 allows you to measure cable delays. Formulas for calculating the current time eliminate delays.
- Accuracy of Local Clocks
  The communication protocol defined by IEEE 1588 takes into account the inaccuracy of local clocks relative to the reference clock. Calculation formulas permit the synchronization of local time, allowing for the inaccuracy of the local clock relative to the reference clock.

The figure illustrates delay and jitter problems when synchronizing clocks.

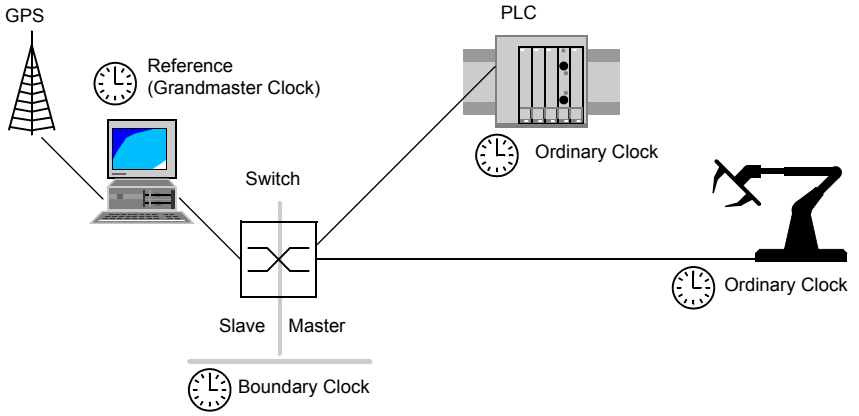


To get around the delay and jitter in the protocol stack, IEEE 1588 recommends inserting a special hardware time stamp unit between the MAC and the PHY layer. Devices or modules with the name supplement **RT** are equipped with a time stamp unit.

The delay and jitter in the LAN increases in the media and transmission devices along the transmission path.

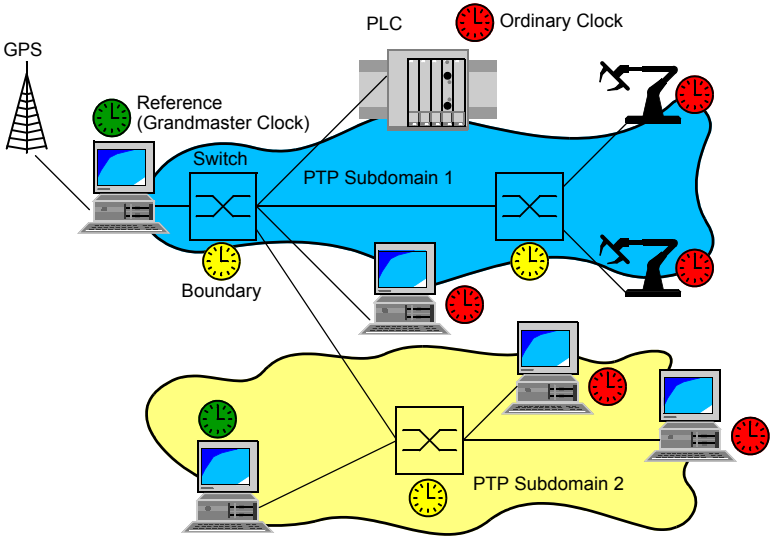
The cable delays are relatively constant. Changes occur very slowly. This fact is taken into account by IEEE 1588. So measurements and calculations are performed on a regular basis.IEEE ignores the inaccuracy caused by device delays and device jitter by defining boundary clocks. Boundary clocks are clocks that are integrated into the devices. These clocks are synchronized on one side of the signal path and, on the other side of the signal path, they are used to synchronize the subsequent clocks (ordinary clocks).

The following figure illustrates how a boundary clock works.



Independent of the physical communication paths, PTP provides logical communication paths you define when you set up PTP subdomains. Subdomains are designed to create groups of clocks that are time-independent of the rest of the domain. Typically, the clocks use the same communication paths that other clocks use.

The following figure illustrates how subdomains work.



Setting Up Your Network and Enabling PTP

You can set up your network and enable PTP as follows:.

Step	Action
1	Draw a network plan showing all devices involved in PTP.
2	Connect all connections you need to distribute PTP information to devices equipped with an integrated time stamp unit (RT modules). Devices which are not equipped with a time stamp unit obtain the PTP information and set their clocks accordingly. They are not involved in the protocol.
3	Connect all devices to Ethernet cables.
4	Open the Web-based interface.
5	Go to **Time** → **PTP**.
6	Select **On** to enable the PTP function on all devices whose time you want to synchronize using PTP.
7	Click **Set** to retain your setting.
8	If there is no reference clock available, designate a switch as reference clock, and set the system time as precisely as possible.

Interaction between PTP and SNTP

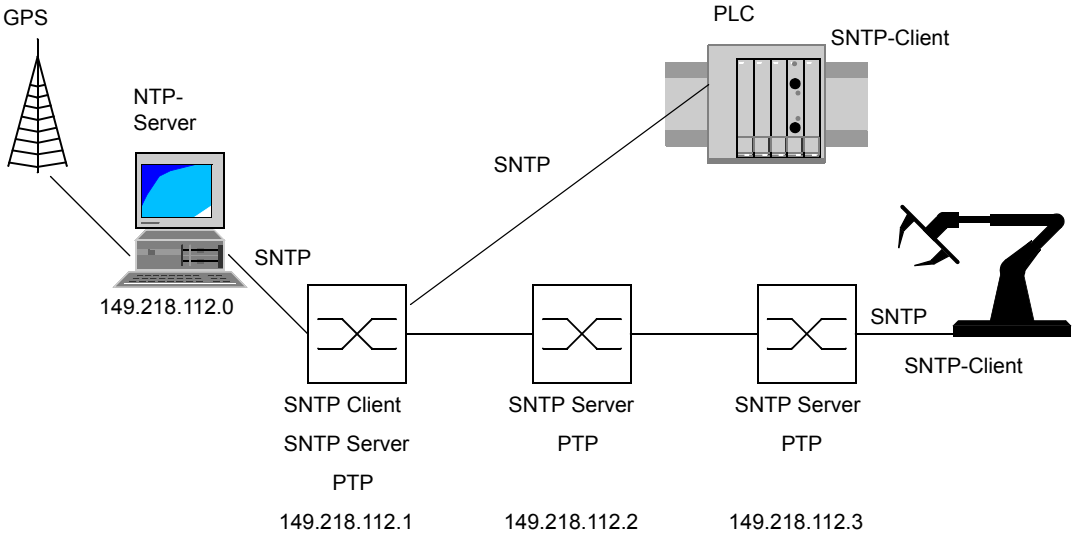
Suggested Configuration of Devices

PTP and SNTP permit each other to coexist in one network. However, since both protocols influence the system time of the device, situations may occur in which they compete with each other.

Note: Configure the devices in such a way that each device receives the system time exclusively from one source. If you want the switch to receive the system time using PTP, enter the external server address 0.0.0.0, and do not accept any SNTP broadcasts when performing the SNTP client configuration. If you want the switch to receive the system time using SNTP, make sure that the best clock is connected to the SNTP server. Thus, both protocols receive the time from the same server.

Application Example

This figure shows an application example of the coexistence of PTP and SNTP.



The requirements made to network time accuracy are rather high, however the end devices exclusively support SNMP, which is less precise than PTP. SNTP achieves an accuracy of milliseconds, whereas PTP has an accuracy of fractions of microseconds (see fig. above).

The following table shows an application example.

Switch	**149.218.112.1**	**149.218.112.2**	**149.218.112.3**
PTP			
Function	On	On	On
Clock Mode	PTP Mode Boundary Clock	PTP Mode Boundary Clock	PTP Mode Boundary Clock
Preferred Master	False	False	False
SNTP			
Function	On	On	On
Anycast Destination Address	224.0.1.1	224.0.1.1	224.0.1.1
Server VLAN ID	1	1	1
Anycast Send Interval	30	30	30
Client External Server Address	149.218.112.0	0.0.0.0	0.0.0.0
Server Request Interval	Any	Any	Any
Accept SNTP Broadcasts	No	No	No

In the example above, the left switch receives as the SNTP client the system time from the NTP server using SNTP. The switch assigns to a time received from an NTP server the stratum clock number 2 (see table on *p. 82*). Thus, the left switch becomes the reference clock for PTP synchronization. PTP is active in all three switches, ensuring that, relative to each other, the system times of the switches are synchronized precisely. As the connectable end devices in the example exclusively support SNTP, all three switches serve as SNTP servers.

Traffic Control

8

At a Glance

Overview

This chapter describes traffic control.

What's in this Chapter?

This chapter contains the following topics:

Directed Frame Forwarding

Directed Frame Forwarding Functions

Directed frame forwarding is a method used by the switch to avoid unnecessary increases in the network load. The switch features the following directed frame forwarding functions:

- store-and-forward,
- multi-address capability,
- static address entries.

Store-and-Forward

All data received by a ESM are stored, and their validity is checked. Invalid and defective tagged frames (> 1522 bytes or CRC errors) as well as fragments (< 64 Bytes) are discarded. Valid tagged frames are forward by the ESM.

Multi-Address Capability

An ESM learns all the source addresses for a port. Only packets with

- unknown addresses
- these addresses or
- a multi/broadcast address

in the target address field are sent to this port.

An ESM can learn up to 4000 addresses. This becomes necessary if more than one end device is connected to one or more ports. It is thus possible to connect several independent subnetworks to an ESM.

Learning Addresses

An ESM monitors the age of the learned addresses. Address entries which exceed a certain age (30 seconds, aging time), are deleted by the ESM from its address table.

Note: A reboot deletes the learned address entries.

Entering the Aging Time in the Web-Based Interface

Enter the aging time as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Switching** → **Global**.
4	Enter the **Aging Time (s)** for all dynamic entries in the range from 10 to 630 seconds (Unit: 1 second, default setting: 30).

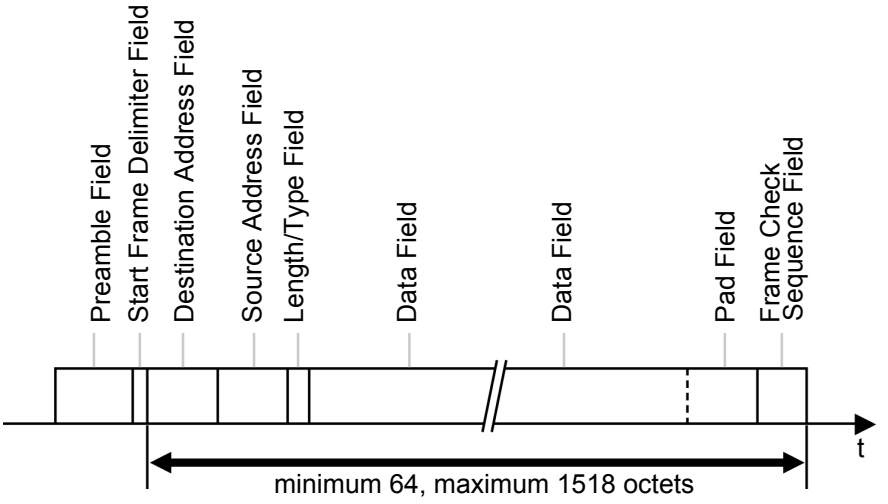
Static Address Entries

One of the most important functions of a switch is the filter function. It selects tagged frames according to certain defined patterns called filters. These patterns are associated with switching rules. This means that a tagged frame received at the port of a switch is compared to the patterns. If no pattern matches the tagged frame, the switch will either transmit or reject the packet according to the switching rules for the affected ports.

The following are valid filter criteria:

- destination address,
- broadcast address,
- multicast address,
- VLAN membership.

The Ethernet tagged frame format is shown in the following figure:



The individual filters are stored in the filter table. The table is divided into three parts, a static part and two dynamic parts.

- The management administrator describes the static part of the filter table (dot1StaticTable).
- During operation, the switch is capable of learning which ports will receive tagged frames from which source addresses. This information is stored in the dynamic part of the table (dot1dTpFdbTable)
- Addresses learned from the neighboring agent and those learned by GMRP are written to another dynamic part.

Addresses already located in the static filter table are automatically transferred by a switch into the dynamic part.

An address entered statically cannot be overwritten through learning.

Note: If the redundancy manager is active, it is not possible to make permanent unicast entries.

Note: In the filtering database, you can create up to 100 filters for multicast addresses.

Multicast Application

Description of Multicast Application

The data distribution in the LAN distinguishes between three distribution classes with reference to the addressed recipient:

- unicast (one recipient)
- multicast (a group of recipients)
- broadcast (every recipient that can be reached)

In the case of a multicast address, switches pass all data packets with a multicast address to all ports in the multicast group. This leads to an increased bandwidth requirement.

Protocols such as GMRP and processes such as IGMP Snooping enable the switches to exchange information by means of the targeted distribution of multicast data packets. The distribution of the multicast data packets exclusively to those ports to which the recipients of these multicast data packets are connected, reduces the bandwidth required.

You can recognize IGMP multicast addresses by the area in which an address is located:

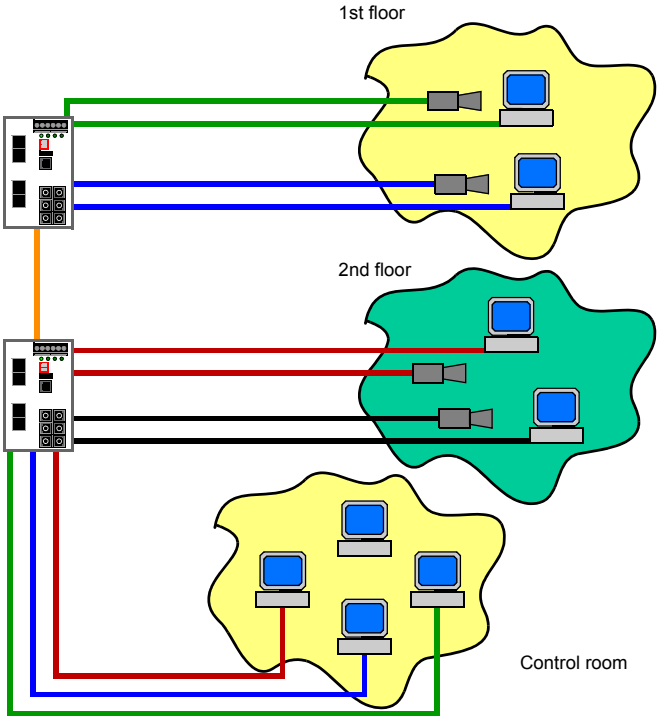
- MAC multicast address (01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF)
- IP multicast address class D (224.0.0.0 - 239.255.255.255)

Example of a Multicast Application

The cameras for machine surveillance normally transmit their images to monitors located in the machine room and in the monitoring room. In an EMS IP transmission, a camera sends its image data with a multicast address over the network.

To prevent the many images from slowing down the entire network, the EMS uses the GMRP to distribute multicast address information. As a result, those images with a multicast address are only distributed to those ports that are connected to the associated monitors for surveillance.

The figure shows a multicast application example.



Description of IGMP Snooping

The Internet Group Management Protocol (IGMP) describes the distribution of multicast information between routers and end devices on layer 3.

Routers with an active IGMP function periodically send queries to find out which IP multicast group members are connected to the LAN.

Multicast group members reply with a report message. This report message contains all parameters required by the IGMP. The router records the IP multicast group address from the report message in its routing table. Then the router transfers frames with this IP multicast group address in the target address field only in accordance with the routing table.

Devices that no longer want to be members of a multicast group can cancel their membership with a Leave message (from IGMP version 2), and they do not transmit any more report messages. In IGMP versions 1 and 2, the router removes the routing table entry if it does not receive any report messages within a specified period of time (aging time). If there are a number of routers with an active IGMP function in the network, then they work out among themselves which router carries out the query function when using IGMP version 2. If there is no router in the network, a suitably equipped switch can carry out the query function.

A switch that connects a multicast receiver with a router can evaluate the IGMP information with the aid of the IGMP Snooping procedure.

IGMP Snooping translates IP multicast group addresses into MAC multicast addresses, so that the IGMP functions can also be used by layer 2 switches. The switch records the MAC addresses of the multicast receivers, which are obtained by the IGMP snooping from the IP addresses, in the static address table. Thus the switch blocks multicast packets at those ports to which no multicast receivers are connected.

Description of GMRP

The GARP Multicast Registration Protocol (GMRP) describes how multicast information is distributed to other switches on layer 2 level. Thus switches can learn multicast addresses. When a multicast address is entered in the static address table, the ESM sends this information to all ports. This tells the connected switches to pass this multicast address on to this switch.

The GARP Multicast Registration Protocol (GMRP) describes the distribution of data packets with a multicast address as the target address. Devices that want to receive data packets with a multicast address as the target address carry out the registration of the multicast address with the aid of the GMRP. For a switch, registration involves entering the multicast address in the filter table. When a multicast address is entered in the filter table, the switch sends this information in a GMRP packet to all the ports. Therefore the connected switches know that they have to send this multicast address to this switch. The GMRP enables packets with a multicast address in the target address field to be sent to the ports entered. The other ports are not affected by these packets.

Data packets with unregistered multicast addresses are sent to all ports by the switch

Default setting: **GMRP enabled**

Devices that do not support GMRP can be integrated into the multicast addressing scheme by means of a static filter address entry on the connector port.

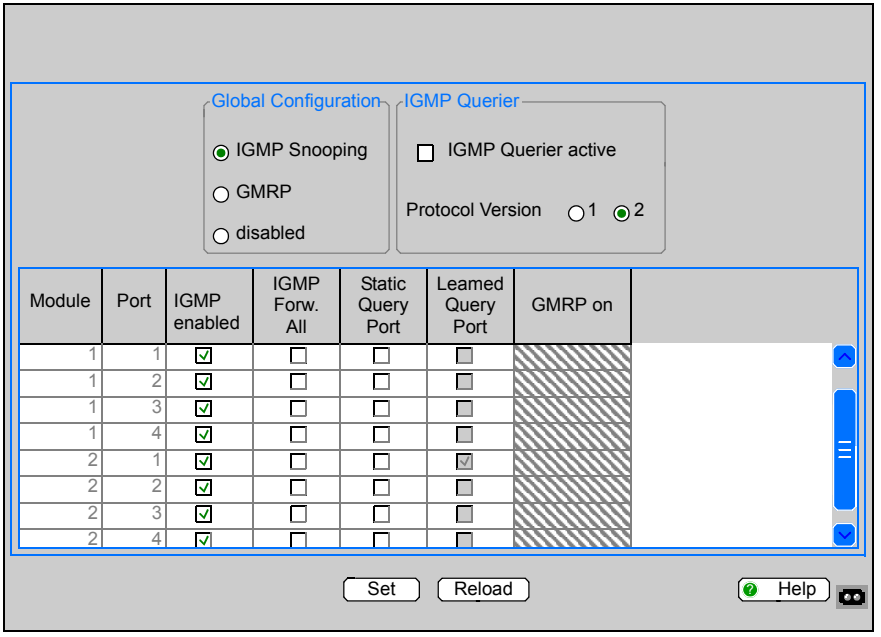
The multicast tree is set up within 5 seconds in a network of up to 20 EMS modules, after the multicast address has been entered for the first time at an EMS port. This time period depends on the *Join Time* that is set (default setting = 200 ms).

Setting Multicast Applications

The remaining blocks of this map explain the setting of multicast applications.

Global IGMP/ GMRP Configuration

Set the multicast applications as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Switching** → **Multicasts**. The following figure shows the **Multicasts** dialog box. 
4	Click the check box to switch **IGMP Snooping** on/off globally for the entire switch. If the IGMP snooping is switched off • the switch does not evaluate query and report packets received, and • it sends (floods) received data packets with a multicast address as the target address to all ports.
5	Click the check box to switch **GMRP** on/off globally for the entire switch. If GMRP is switched off • the switch does not generate any GMRP packets, • the switch does not evaluate any GMRP packets received, and discards them, • it sends (streams) received data packets with a multicast address as the target address for all ports. The switch is transparent for received GMRP packets, regardless of the GMRP setting.

Individual IGMP/ GMRP Configuration

The blocks below explain the individual IGMP/GMRP configuration.

IGMP Querier

With **IGMP Querier Active** you can switch the query function on/off.

The protocol check boxes allow you to select IGMP version 1 or version 2.

IGM Enabled per Port

This table column enables you to switch on/off the IGMP for each port when the global IGMP is switched on. When you switch off the IGMP at a port, no registrations can be made for this port.

IGM Forward All per Port

This column of the table allows you to switch on/off the IGMP Snooping function when the global IGMP Snooping is switched on. With the forward all setting, the switch forwards all the data packets with a multicast address in the target address field to this port.

Note: If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.

Note: If a number of routers are connected to a subnetwork, you must use IGMP version1, so that all the routers receive all the IGMP reports.

Static Query Port

A switch sends IGMP report messages to the ports at which it receives IGMP queries. This column allows you to also send IGMP report messages to other selected ports.

Learned Query Port

A switch sends IGMP report messages to the port at which it receives IGMP queries. This column displays the ports on which the switch has received IGMP queries.

GMRP per Port

This table column enables you to switch on/off the GMRP for each port when the global GMRP is switched on. When you switch off the GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be sent out of this port.

Note: If the switch is connected to a HIPER ring, you can ensure in case of a ring interruption quick reconfiguration of the network for data packets with registered multicast target addresses by:

- switching on the IGMP both at the ring port and globally, and
- switching on the **IGMP Forw. All** per port on the port rings.

The Broadcast Limiter

Description of the Broadcast Limiter

To guarantee reliable data exchange during high broadcast traffic, the switch can limit broadcast traffic.

By entering a number for each port, you can set the number of broadcasts that can be sent out of this port within a second.

If more than the maximum entered number of broadcasts are sent within a second, the switch rejects all subsequent broadcasts destined for this port.

A global setting activates/deactivates the broadcast limiter function at all ports

Setting the Broadcast Limiter in the Web-Based Interface

Step	Action	Comment
1	Connect the ESM to an Ethernet cable.	
2	Open the Web-based interface.	
3	Go to **Switching** → **Broadcast Limiter** to set the options per port.	In the check box, you can switch on and off the broadcast limiter for all ports.
4	Enter a number of broadcast for each port.	• =0, no limitation on the broadcasts out of this port. • >0, maximum number of broadcasts that can be sent out of this port.

Prioritization

Descripton of Prioritization

This function prevents high-priority data traffic from being disrupted by other traffic during busy periods. Low-priority traffic is discarded when the memory or transmission channel is overloaded.

The EMS supports four priority queues (traffic classes in compliance with IEEE 802.1D-1998). The assignment of received data packets to these classes depends on

- the priority of the data packet contained in the VLAN tag (priority over port priority),
- the priority for receiving the data packets that do not contain a tag (see *p. 59*).

Assignment of Priorities

The assignment of the priority number to the four priority classes is as follows:

Entered Priority	Priority Class
0	1 - normal
1	0 - low
2	0 - low
3	1 - normal
4	2 - high
5	2 -high
6	3 - admin
7	3 - admin

Strict Priority

With strict priority, the switch send all data packets with a higher priority level before it sends a data packet with the next lower priority level. Thus, the switch does not send a data packet with the next lower priority level until there are no other data packets waiting in the queue.

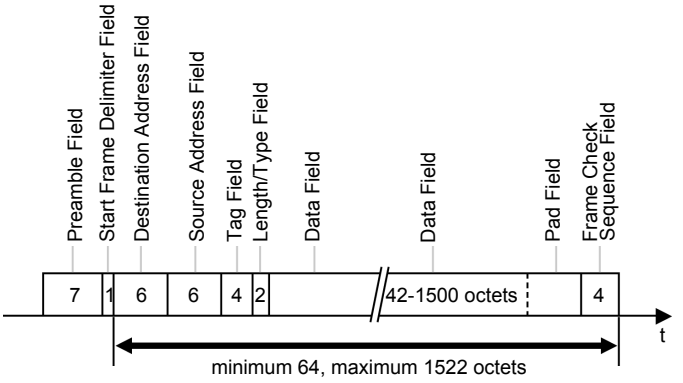
Tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and prioritization functions in accordance with the IEEE 802.1 Q standard. The VLAN tag consists of 4 Bytes. It is inserted between the source address field and the type field.

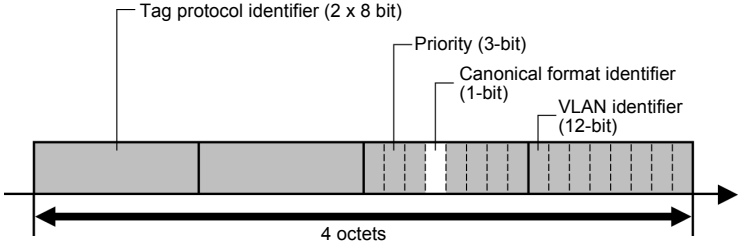
With VLAN-tagged frames, the switch evaluates:

- the priority information at all times,
- the VLAN information, if VLANs have been set up.

Frames with VLAN tags that contain priority information but no VLAN information (VLAN ID = 0) are called priority tagged frames. An Ethernet tagged frame with one such tag is shown in the following figure:



The tag format is shown in the following figure:



Setting Prioritization Using the Web-Based Interface

Set the Prioritization as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Port Configuration**. Specify in the **Port Priority** column the priority (low, normal, high, admin) with which the switch sends data packets which it receives without a VLAN tag at this port.

Flow Control

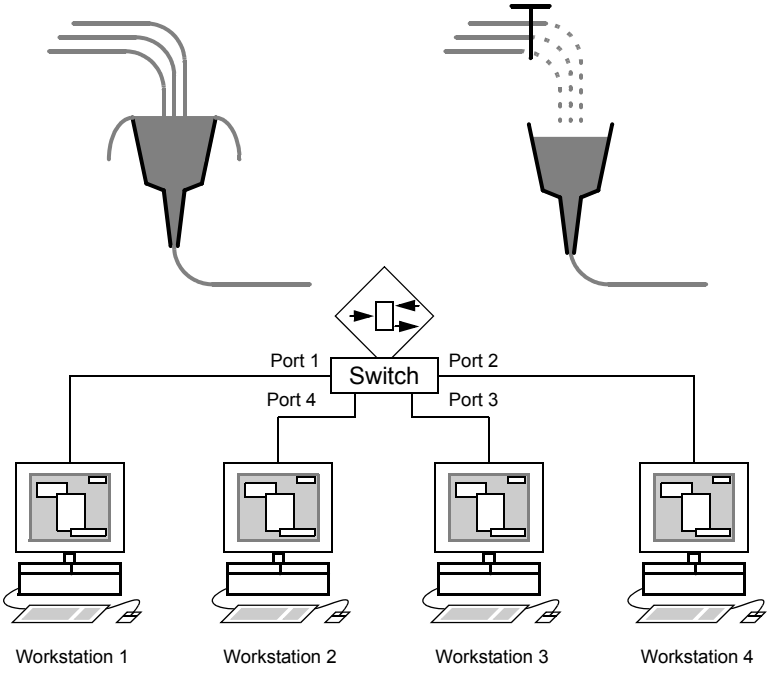
Description of Flow Control

Flow control is a mechanism which acts as an overload protection. During periods of heavy traffic it holds off additional traffic.

In the example below, the functioning of flow control is displayed graphically. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to workstation 4. The combined bandwidth of Workstations 1, 2 and 3 is larger than the bandwidth of workstation 4 to the switch. This leads to an overflow of the send queue of port 4. The left-hand funnel symbolizes this status.

If the flow control function at ports 1, 2 and 3 of the switch is turned on, the switch reacts before the funnel overflows. Ports 1, 2 and 3 send a message to the connected devices that no data may be received at present.

The following figure shows a flow control example:



Full Duplex Link

In the above example there is a full duplex link between workstation 2 and the switch. Before the send queue of Port 4 overflows, the switch sends a request to workstation 2 to include a small break in the sending transmission.

Half Duplex Link

In the above example there is a half duplex link between workstation 2 and the switch. Before the send queue of port 4 overflows, the switch sends data so that workstation 2 detects a collision and thus interrupts the transmission.

Setting Flow Control in the Web-Based Interface

You can set flow control as follows in the web-based interface.

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Basics** → **Port Configuration**.
4	Enable flow control for a particular port by checking **Flow Control** for the appropriate port number.
5	Go to **Switching** → **Global**. This dialog enables you to ● switch off flow control at all ports, or ● switch on flow control at all ports which have been selected for flow control in the configuration table.

Description of VLANs

VLANs

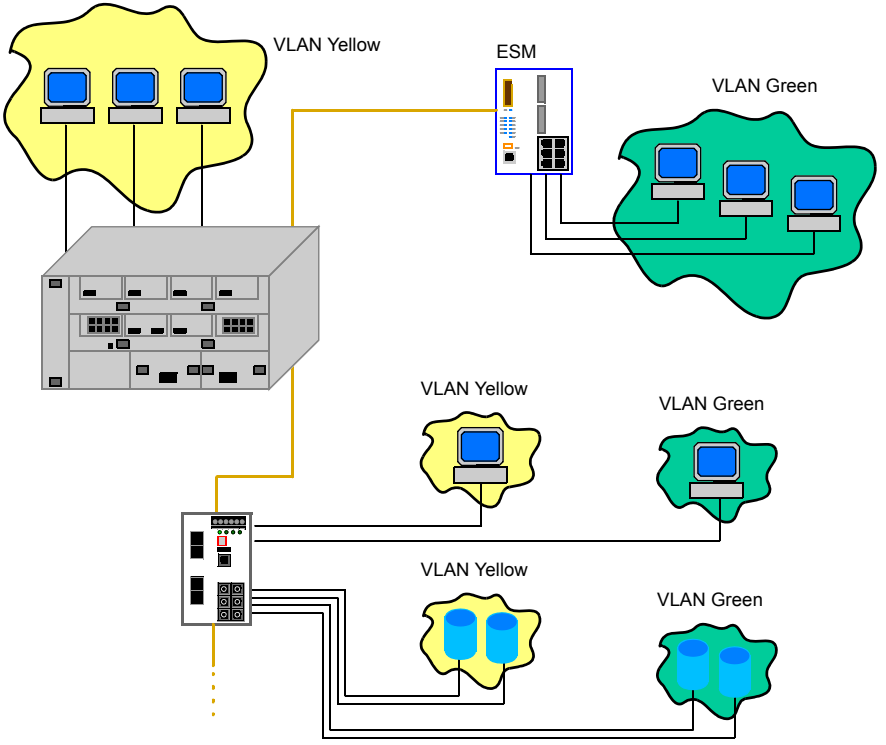
A virtual LAN (VLAN) consists of a group of network subscribers in one or more network segments which can communicate with each other as if they belonged to the same LAN.

VLANs are based on logical (instead of physical) links and are flexible elements in the network design. The biggest advantage of VLANs is the fact that they permit the formation of user groups based on their subscriber function and not on their physical location or medium.

Since broadcast/multicast data packets are transmitted exclusively within a virtual LAN, the remaining data is not affected.

The VLAN function is defined in the IEEEE 802.1Q standard. The maximum number of VLANs is limited by the structure of the VLAN tag to 4094 (see figure in *p. 98*).

The following figure shows a VLAN application example.



VLAN Keywords

Keywords used in association with VLANs are:

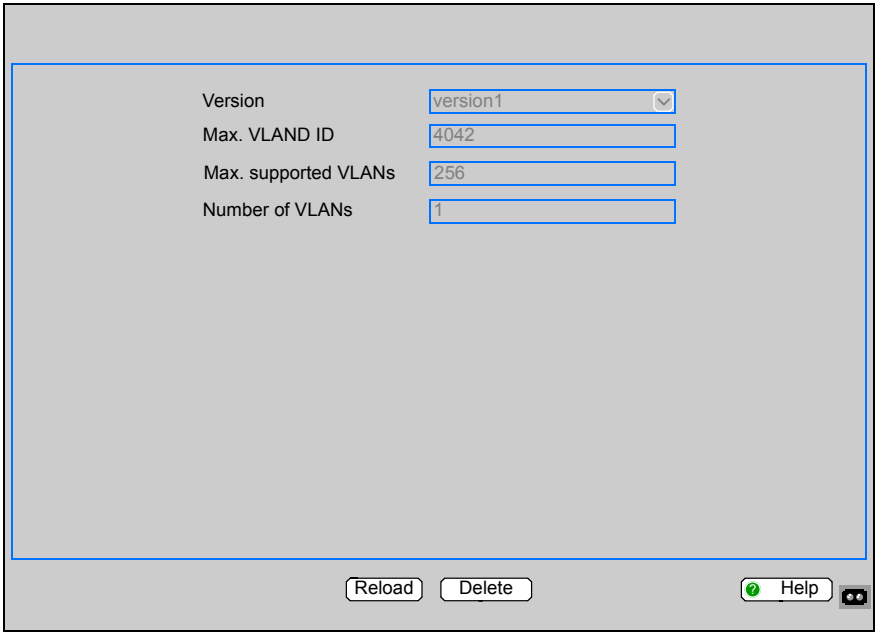
- Ingress Rule
  Ingress rules stipulate how incoming data are to be handled by the switch.
- Egress Rule
  Egress rules stipulate how outgoing data are to be handled by the switch.
- VLAN Identifier
  The assignment to a VLAN is executed using VLAN ID. Every VLAN in a network is identified with an ID which must be unique, i.e. every ID may only be assigned once in the network.
- Port VLAN Identifier (PVID)
  The management assigns a VLAN ID for every port. Thus, it is known as the port VLAN ID.
  The switch adds a tag to every packet received without a tag. This tag contains a valid VLAN ID.
  When a data packet is received with a priority tag, the switch adds the port VLAN ID.
- Member Set
  The member set is a list of ports belonging to a VLAN.
  Each VLAN has a member set.
- Untagged Set

The untagged set is a list of the ports of a VLAN which send data packets without a tag. Every VLAN has an untagged set.

Configuring VLANs

Configuration Procedure Using the Web-Based Interface

Configure VLANs as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go the **Switching** → **VLAN** → **Global**. The figure shows the **VLAN Global** dialog box.  Under VLAN you will find all tables and attributes to configure and monitor the VLAN functions complying with IEEE 802.1Q standard. **Note:** When configuring VLAN, ensure that the port to which your management station is connected can still send data of the management station after saving the VLAN configuration. If you assign the port to the VLAN with ID 1, you can always ensure that the management station data can be sent. To set up VLANs, you first specify the desired VLANs in the desired static VLAN table (Static). After setting up VLANs, you specify the rules for received data in the port table (Port).
4	Use the **Delete** button to restore all the default VLAN settings of the device (default settings).
5	Save the VLAN configuration to ensure it is effective after restart and then restart the switch.

Note: The 256 VLANs available can use any VLAN ID in the range of 1 to 4042.

Note: In the HIPER ring with VLANs, you should select only operate devices with the software that supports this function.

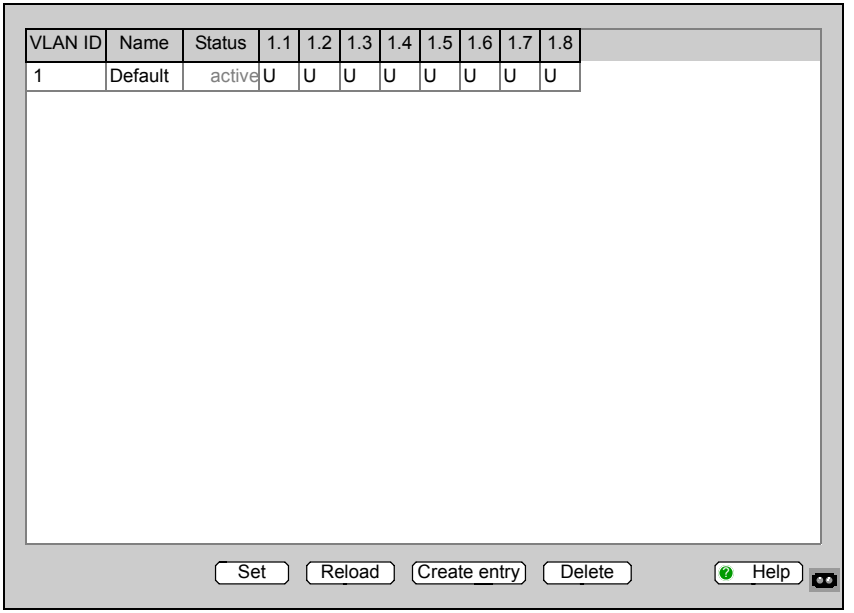
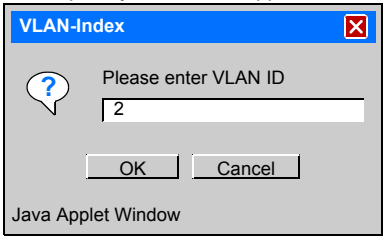
Note: In the HIPER ring configuration, select for the ring ports:
- VLAN ID 1 and **Ingress Filtering** are disabled in the port table, and
- VLAN affiliation **U** in the static table.

Note: In the Ring/Network coupling configuration, select for the coupling and partner coupling ports:
- VLAN ID 1 and **Ingress Filtering** disabled in the port table, and
- VLAN affiliation **U** in the static table.

Setting up VLANs

Setting up Procedure Using the Web-Based Interface

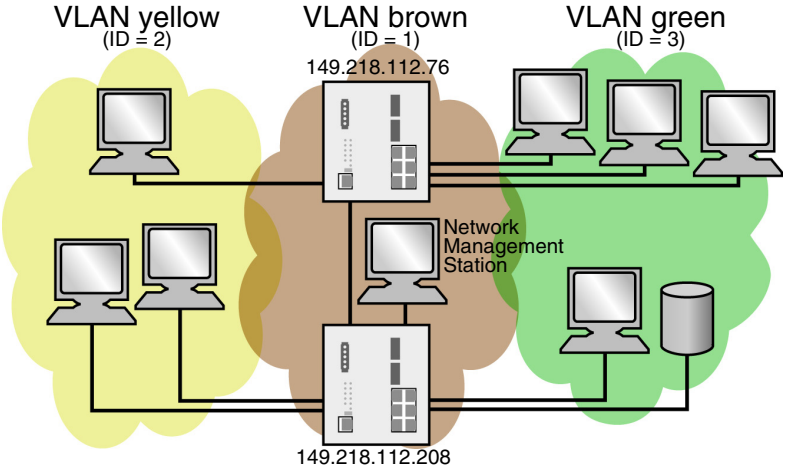
Set up VLANs as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Switching** → **VLAN** → **Static**. The following dialog box appears. 
4	Click **Create**, and enter the appropriate VLAN ID in the dialog box shown below: Subsequently, a new line appears in the table. 

Step	Action
5	Enter the name of you choice for this VLAN.
6	Define in the dialog box shown below the affiliation of the ports you require, and save your settings by pressing **Set**. You can choose from the following options: ● **-**: not a member of the VLAN ● **M**: a member of the VLAN (packet is transmitted with a tag ● **F**: not a member of the VLAN ● **U**: a member of the VLAN (packet is sent without a tag) For the following explanation, refer also to the section **Simple VLAN Example** below. Ports 1 to 3 are assigned to the end devices of the yellow VLAN and ports 4 to 5 to the end devices of the green VLAN. As end devices normally do not sent data packets with a tag, the setting `U` must be selected here. Port 6 serves as uplink port to the next switch. It is assigned the setting `M`. The VLAN information can thus be passed on.

Simple VLAN Example

This example reflects a standard implementation of the EMS in a simple VLAN configuration:



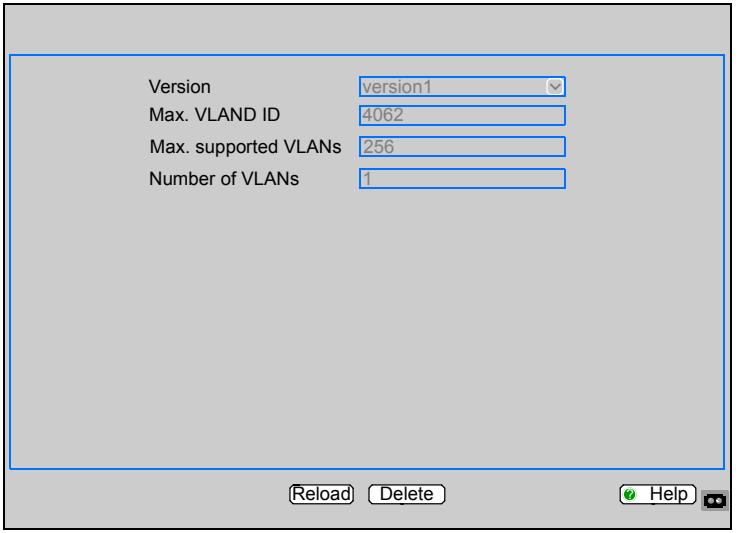
Specifying Rules for Data Received

After setting up VLANs, specify the rules for data received as follows:

Step	Action
1	Go to **Switching** → **VLAN** → **Port**.
2	Specify the rules for data received in the port table. ● **VLAN ID** - specifies to which VLAN a received untagged data packet is assigned to. ● **Acceptable Frame Types**- determines whether data packets can also be received untagged. ● **Ingress Filter**- specifies whether the received tags are evaluated.
3	To save the settings you have made, press **Set**.

Viewing and Deleting the VLAN Settings

Delete the VLAN settings as follows:

Step	Action
1	Go to **Switching** → **VLAN** → **Current** to view the settings. The table displays all VLANs configured.
2	Go to **Switching** → **VLAN** → **Global**. In the dialog box shown below, press the **Delete** button to restore all the VLAN settings of the device to default settings. 
3	Go to **Switching** → **VLAN** → **Static**.
4	Press the **Delete** button in this dialog to delete a selected row in the table.

Operation Diagnostics

9

At a Glance

Overview

This chapter describes the diagnosis tools of your switch.

What's in this Chapter?

This chapter contains the following topics:

Sending Traps

SNMP Traps

If unusual events occur during normal operation of the ESM, they are reported immediately to the management station. This is done by means of so-called trap alarms that bypass the polling procedure. (**Polling** means to query the data stations in regular intervals). Traps make it possible to react quickly to critical situations.

Examples for such events are:

- hardware reset
- changing the basic device configuration
- segmentation of a port

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.

The management agent sends traps to those hosts that are entered in the target table (trap destination table). The trap destination table can be configured with the management station via SNMP.

SNMP Trap Listing

All possible traps that can occur are listed in the following table.

Trap Description	A trap is sent if....
authenticationFailure	A station attempts to access an agent without permission.
coldStart	A cold and warm start occurs during the boot process after successful management initialization.
saMemoryBackupAdapterTrap	The Memory back up adapter is inserted or removed.
linkDown	The link to a port breaks.
linkUp	The link to a port is re-established.
saTemperature	This alarm message is sent if the temperature exceeds the limit set.
saPowerSupply	The status of the voltage supply changes.
saSignallingRelay	The status of the signal contact changes.
newRoot	The sending agent becomes the new root of the spanning tree.
topologyChange	The transmission mode of a port changes.
risingAlarm	An RMON alarm input exceeds the upper threshold.
fallingAlarm	an RMON alarm input falls below the lower threshold.

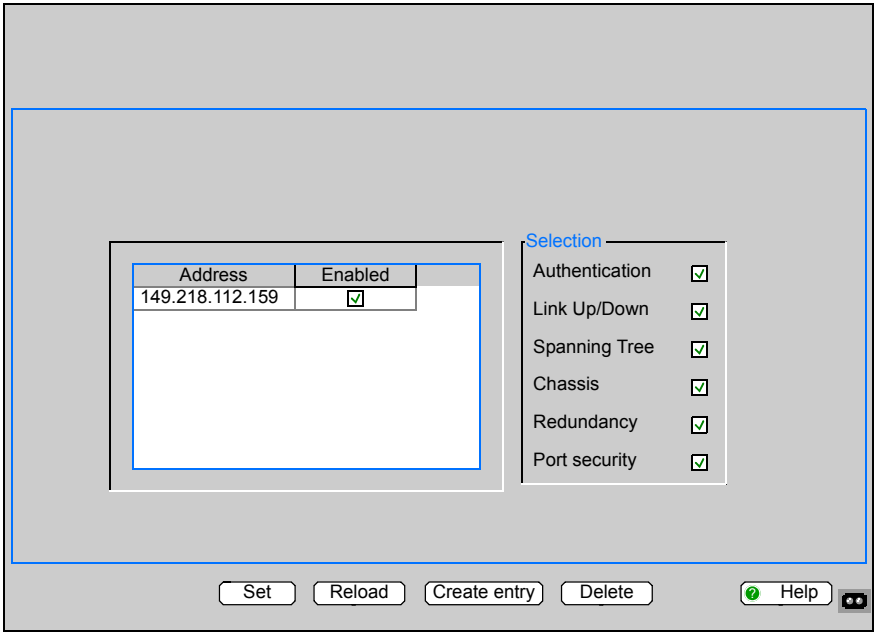
Trap Description	A trap is sent if....
saPortSecurityTrap	A MAC address is detected at the port which does not correspond to the current settings of: • `saPortSecPermission` and • `saPorSecAction` set either to `trapOnly` (2) or `portDisable` (3).
saModuleMapChange	The hardware configuration has changed.
saBDPUGuardTrap	A BPDU is received at a port although the BPDU guard function is activated.
saRingRedReconfig	when the configuration of the redundant ring changes.
saRingRedCplReconfig	The configuration of the redundant ring/network coupling changes.
saSNTPTrap	Errors occur in connection with the SNTP protocol (e.g., server not available).
saRelayDuplicateTrap	A duplicate IP address is detected in connection with the DHCP Option.
lIdpRemTablesChangeTrap	This alarm message is sent if an entry in the topology table changes.

SNMP Traps when Booting

Note: The trap coldStart is sent during every boot procedure.

Configuring Traps Using the Web-Based Interface

Configure the traps as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Diagnostics** → **Alarms (Traps)**. Access this dialog with the read-write password. The **Alarms (Traps)** dialog allows you to specify both the events triggering an alarm (trap) and the persons these alarms should be sent to. This figure shows the **Alarms (Traps)** dialog box. 
4	In the **IP Address** column, enter the IP address of a network management station which the traps should be sent to.
5	In the **Enabled** column, mark the entries which should be taken into account when traps are being sent.
6	In the **Selection** group box, check the trap categories from which you want to send traps.

Selecting Events Triggering an Alarm

You can have an alarm triggered in case of the following events by selecting them in the **Selection** group box of the **Alarms (Traps)** dialog box.

Event	Description
Authentication	The switch has rejected an unauthorized access attempt (see **Access for IP Addresses** and **Port Security** dialog).
Cold Start	The switch has been turned on.
Link Up	The link to the device at one port of the switch has been established.
Link Down	The link to the device at one port of the switch has been interrupted.
Spanning Tree	The topology of the **Rapid Spanning Tree** has changed.
Chassis	Chassis encompasses the following events: • **Power Supply**: The status of a supply voltage has changed (see **System** dialog box. • **Signal Contact:**: The status of the signal contact has changed. To follow the event, go to **Signal Contact**, and select **generate Trap**. • **Media Module**: A media module has been added or removed. • **Memory back up adapter**: The Memory back up adapter has been inserted or removed. • **Temperature**: The value has been exceeded / fallen below the temperature threshold.
Redundancy	The status of the HIPER ring or the redundant coupling of HIPER rings/ network segments has changed.
Port Security	A data packet has been received on one port from an unauthorized end device.

Contact Signal

Description of the Contact Signal

The signal contacts are for:

- controlling external devices by manually setting the signal contacts,
- monitoring proper functioning of the ESM which makes it possible to perform remote diagnostics.

By means of the potential-free signal contact (relay contact, closed circuit) a contact break is reported. This can be due to:

- faulty power supply:
  the failure of the supply voltage 1/2,
  power supply voltage 1 or 2 < 18 V
  a continuous malfunction in the ESM (internal 3.3 VDC voltage),
- values that exceed or fall below the set temperature threshold,
- removing a module,
- removing the back up configuration adapter,
- the defective link status of at least one port
  With the ESM, the displaying of the link status can be masked by the management for each port (see *p. 62*). The link status is not monitored in the default settings.
- HIPER ring event:
  the loss of redundancy guarantee (in redundancy manager mode). The Ring redundancy monitoring default setting is **monitoring turned off**.
- redundant ring/net coupling event:
  the loss of redundancy guarantee. Ring redundancy monitoring default setting is **monitoring turned off**. In Stand-by mode the ESM reports additionally the following conditions:
  - the faulty link status of the control line,
  - partner device in stand-by mode.

  The management setting determines which events causes a contact to the ESM.

Note: With non-redundant supply of the mains voltage, the EMS reports a power failure. You can prevent this message by applying the supply voltage over the two inputs or by switching off the monitoring function.

Manually Setting the Signal Contact

This mode enables you to carry out the remote switching of each signal individually. You have the following applications options:

- simulating an error during PLC error monitoring,
- remote controlling a device using SNMP, for instance switching on a camera.

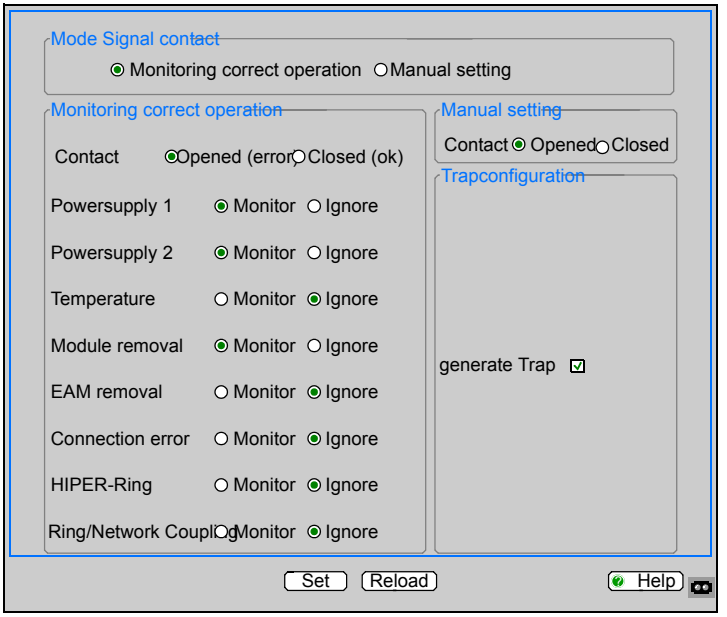
Setting Up Procedure Using the Web-Based Interface

Set the signal contact as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Diagnostics** → **Signal Contact**.
4	Click **Manual setting** in the **Mode Signal contact** frame to set contact to manual.
5	Click **Opened** in the **Manual Setting** group box to open the contact.
6	Click **Closed** in the **Manual Setting** group box to close the contact.

Configuring the Signal Contact for Monitoring Correct Operation in the Web-Based Interface

Configure the signal contact as follows:

Step	Action
1	Go to **Diagnostics** → **Signal Contact**. The dialog below appears. 

Step	Action
2	In the **Mode Signal contact** group box, select **Monitoring correct operation** to use the contact for function monitoring.
3	In the **Monitoring correct operation** group box, select the events which you want to have monitored.
4	For temperature monitoring, go to **Basics** → **System**.
5	In the line **Temperature (°C)** of the **System Data** group box, set the temperature thresholds to be monitored.

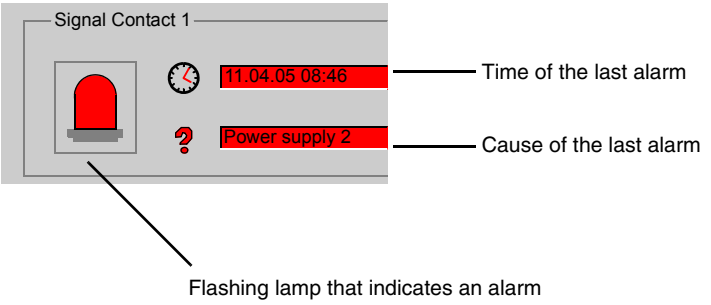
Displaying the Signal Contact

You can view the signal contact state in three ways:

- using the LED display,
- using the web-based interface,
- executing a query in the command line interface.

Alarm

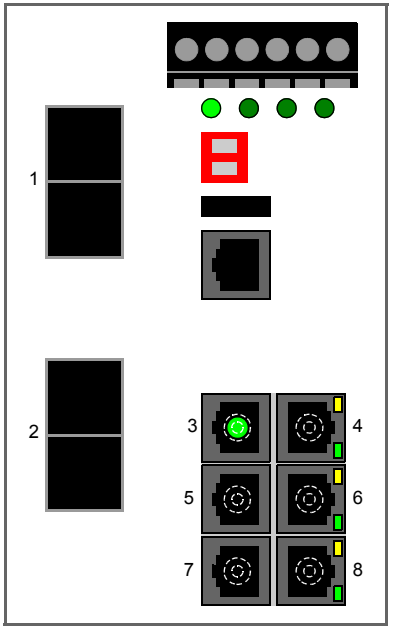
This portion of the home page provides information on the alarm state of the ESM.



Displaying the Port Status

Procedure Using the Web-Based Interface

You can dispaly the port status as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-Based interface.
3	Go to **Basics** → **System**. The figure below shows the device view. 
4	Point the mouse arrow at the symbols for the individual ports at the bottom of the screen. As a result, a box will appear which indicates the port status and other port-related information.

Event Counter on Port Level

The Port Statistics Table

The port statistics table allows experienced network administrators to identify possible problems occurring in the network.

This table shows you the contents of various events counters. After a restart, all the event counters begin at zero. The counters add up the events which have been transmitted and received.

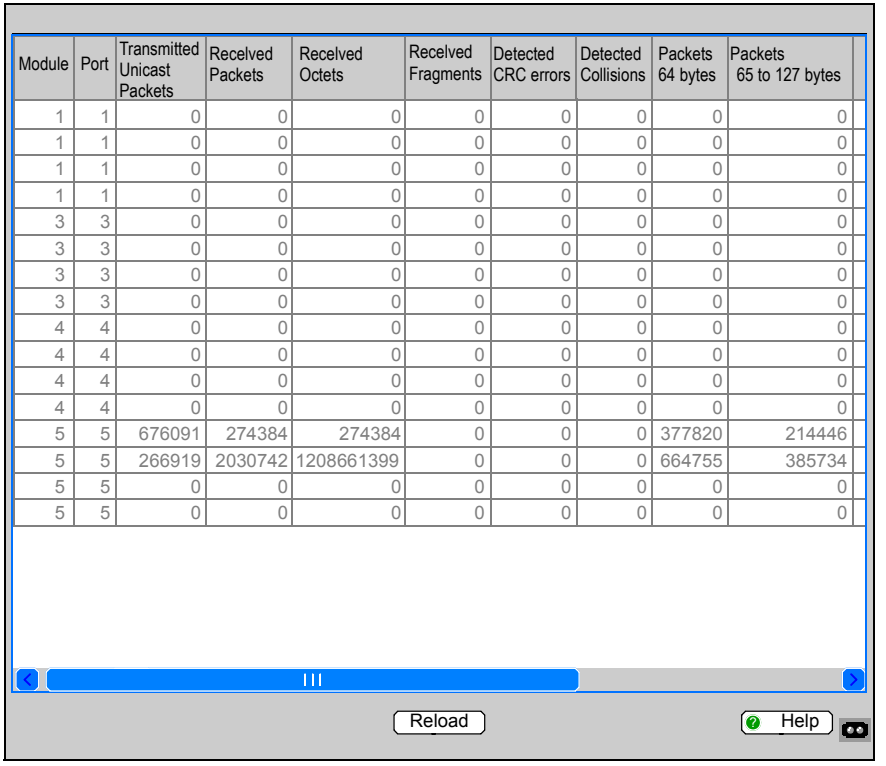
The following table explains the content of various event counters.

Counter	Possible Problems
Received Fragments	• The controller of the connected device is faulty. • Electromagnetic interference is injected into transfer medium.
CRC Errors	• The controller of the connected device is faulty. • Electromagnetic interference is injected into the transfer medium. There is a faulty component in the network.
Collisions	• The controller of the device is faulty. • The network expansion is too big or the line is too long. • A packet has collided with an interference signal.

Opening the Statistics Table Dialog in the Web-Based Interface

Open the statistics table as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Diagnostics** → **Ports** → **Statistics**. The figure shows the **Statistics** table.



Module	Port	Transmitted Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Packets 64 bytes	Packets 65 to 127 bytes
1	1	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0
3	3	0	0	0	0	0	0	0	0
3	3	0	0	0	0	0	0	0	0
3	3	0	0	0	0	0	0	0	0
3	3	0	0	0	0	0	0	0	0
4	4	0	0	0	0	0	0	0	0
4	4	0	0	0	0	0	0	0	0
4	4	0	0	0	0	0	0	0	0
4	4	0	0	0	0	0	0	0	0
5	5	676091	274384	274384	0	0	0	377820	214446
5	5	266919	2030742	1208661399	0	0	0	664755	385734
5	5	0	0	0	0	0	0	0	0
5	5	0	0	0	0	0	0	0	0

Resetting Port Counters Using the Web-Based Interface

Reset port counters as follows:

Step	Action
1	Go to **Basics** → **Restart**.
2	Click **Reset port counters**.

Displaying the SFP Status

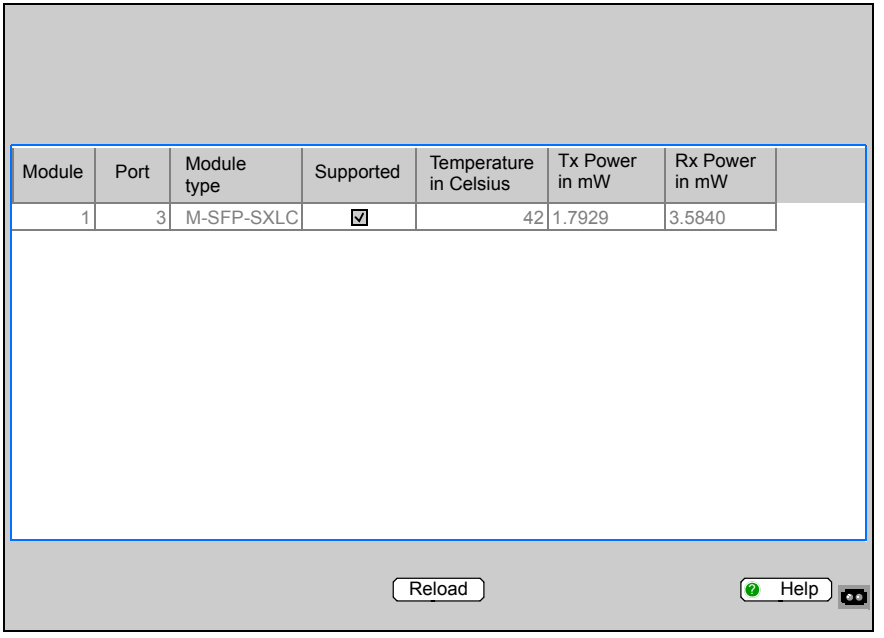
Properties of SFP Modules

By having the SFP status displayed, you can view the current connection to the SFP modules and their properties. The properties include:

- module type
- support provided in the media module
- temperature in degrees Celsius
- transmission power in mW
- reception power in mW

Opening the SFP Module Dialog Box in the Web-Based Interface

Open the SFP dialog box as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Diagnostics** → **Ports** → **SFP modules**. The figure shows the SFP module dialog box. 

Topology Discovery

Description of Topology Discovery

IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP).

LLDP allows users to automatically detect the topology of their LANs. A device with active LLDP

- sends its own connection and management information to neighboring devices of the shared LAN if they have LLDP activated,
- receives connection and management information from neighboring devices of the shared LAN if they have LLDP activated,
- and sets up a management information scheme and object definitions for saving connection information of neighboring devices that have LLDP activated.

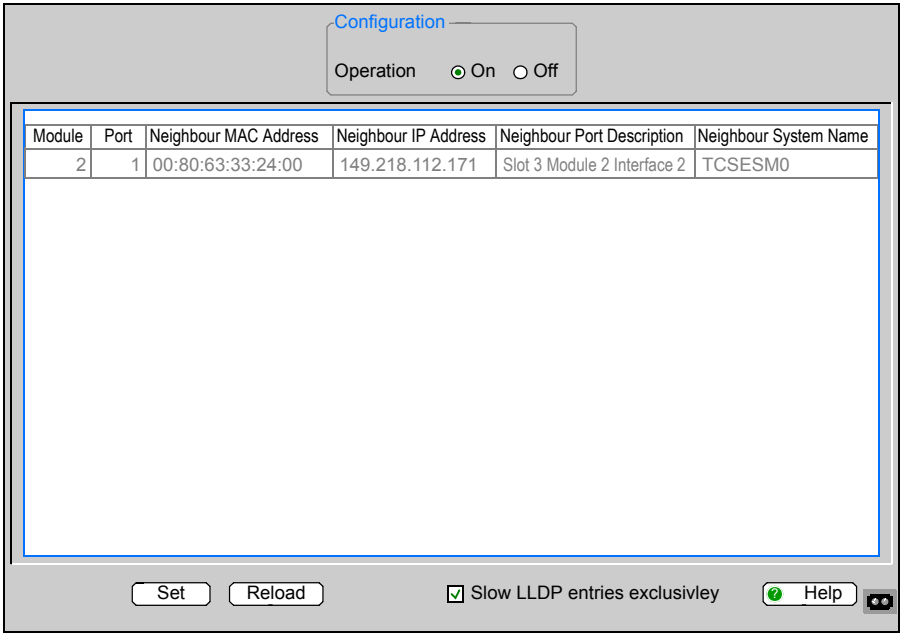
The connection information contains as its most significant element the precise and unique ID of a connection endpoint: MSAP (MAC Service Access Point). This is composed of the MAC address of the device and a port ID that is unique to this device.

The contents of the connection and management information are:

- chassis ID (its MAC address)
- port ID (its port MAC address)
- description of the port
- system name
- system description
- currently activated **system capabilities**
- Interface ID of the management address
- VLAN-ID of the port
- status of autonegotiation on the port
- medium, half/full duplex setting and transmission speed setting of the port
- information about the redundancy protocol (STP, RSTP, HIPER ring, ring coupling, dual homing) activated at this port
- VLAN information concerning the port (VLAN ID and VLAN name)
  This information can be called up from a network management station. With this information, the network management station is able to display the topology of the network.
  LLDP uses an IEEE-MAC address for exchanging information. This address is normally not routed by switches. This is why switches without LLDP support drop the LLDP packets. Consequently, a non-LLDP-capable device between two LLDP-capable devices prevents the exchange of LLDP information.To avoid this, ESM Switch send additional LLDP packets to the ESM Multicast-MAC address 01:80:63:2F:FF:0B. ESM Switch with the LLDP function are thus also able to exchange LLDP information with each other via devices which themselves are not LLDP-capable.
  The Management Information Base (MIB) of an LLDP capable ESM Switch holds out the LLDP information in the lldp-MIB and in the private salldp-MIB.

Displaying Topology Discovering the Web-Based Interface

Display topology discovery as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Diagnostics** → **Topology Discovery**. The table shows you the selected information to neighbor devices. 
4	Click **Show LLDP entries exclusively** to reduce the number of topology table entries. In this case, the topology table hides entries of devices without active topology discovery function.

Explanation concerning the Topology Discovery Dialog Box

If several devices are connected to a port, for example via a switch, the table shows one line for each connected device.

If

- devices with active topology discovery function and
- devices without active topology discovery function

are connected to a port, the **Topology Discovery** table hides the devices without active topology discovery.

If

- only devices without active topology discovery are connected to a port, the table will contain one line for this port symbolically for all devices.
  MAC addresses of devices that the **Topology Discovery** table hides for the sake of clarity, are located in the **Address** table (see *p. 89*).

Reports

Explanation of the Various Report Types

For diagnosis purposes, the ESM allows you to use the following reports:

- Log File
  The Log File is an HTML file in which the ESM records all important switch internal events.
- System Information
  The system information in an HTML file containing all system relevant data. These reports provide technicians with the information required for servicing the ESM.

Viewing and Sending the Reports Using the Web-Based Interface

Proceed as follows to view and open the reports:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Diagnostics** → **Reports**. A window is opened which shows the following links: • **Log File** • **System Information**
4	Click **Log File** to open the HTML file in a new browser window.
5	Click **System Information** to open the HTML file in a new browser window.

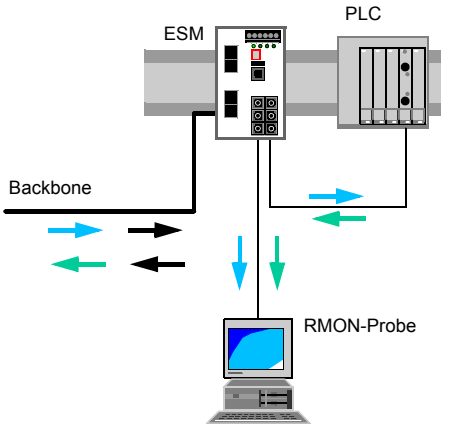
Monitoring Port Traffic

Port Mirorring

In port mirroring, data traffic related to one port (the source port) is copied to another (the destination port). Data traffic at the source port is not influenced by port mirroring. A management tool connected to the destination port, like an RMON probe, can observe data traffic at the source port.

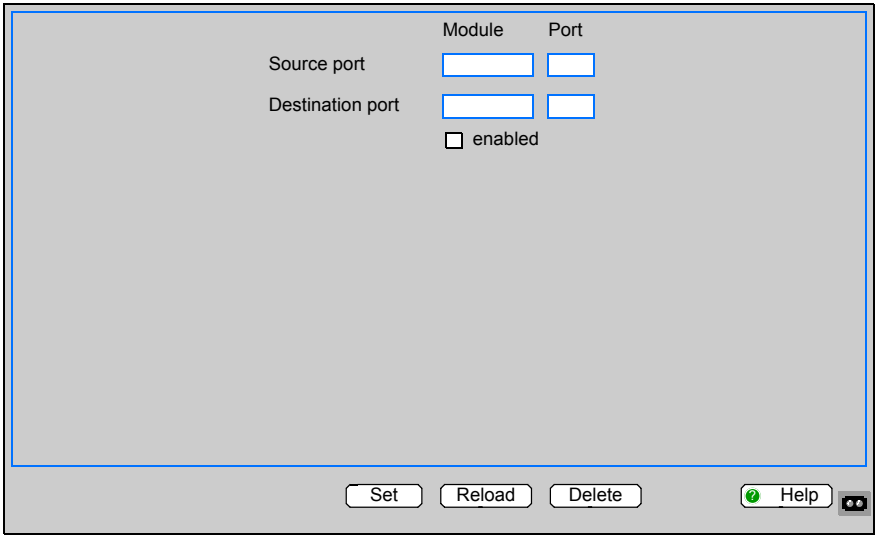
The destination port forwards data to be sent and blocks received data.

Port monitoring is shown in the figure below:



Monitoring Port Traffic

Monitor port traffic as follows:

Step	Action
1	Connect the ESM to an Ethernet cable.
2	Open the Web-based interface.
3	Go to **Diagnostics** → **Port Mirroring**. The window below appears. 
4	Select the source port whose data traffic you wish to monitor.
5	Select the destination port to which you have connected your management tool.
6	Click **enabled** to enable the function.

Appendices

At a Glance

What's in this Appendix?

The appendix contains the following chapters:

General Information

A

At a Glance

Overview

This chapter provides general information concerning the ESM.

What's in this Chapter?

This chapter contains the following topics:

The Management Information Base (MIB)

MIB Description

The Management Information Base (MIB) is designed in the form of an abstract tree structure.

The branching points are the **object classes**. The leaves of the MIB are called **generic object classes**. Wherever necessary for unambiguous identification, the generic object classes are **instantiated**, i.e. the abstract structure is imaged on the reality, by specifying the port address or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances. These values can be read and, in some cases, modified. The **object description** or **object ID** (OID) identifies the object class. The subidentifier (SID) is used for instantiation.

Example:

The generic object class

`saPSState (OID = 1.3.6.1.4.1.3833.1.1.14.1.2.1.3)`

is the description of the abstract information power supply state. It is, however, not possible to read any information from this, as the system does not know which power supply is meant.

Specification of the subidentifier (2) images this abstract information on the reality (instantiates it), which means that it refers to power supply 2. A value is assigned to this instance and can then be read.

The instance **get** `1.3.6.1.4.1.248.14.1.2.1.3` **2**, for example, returns the response **1**, which means that the power supply is ready for operation.

MIB Abbreviations

The following table defines the abbreviations used in the MIB.

Abbreviation	Meaning
Comm	Group access rights
Con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g., threshold)
PS	Power supply
Pwr	Supply voltage
sys	System
UI	User Interface
Upr	Upper (e.g., threshold)
ven	Vendor (Schneider Electric)

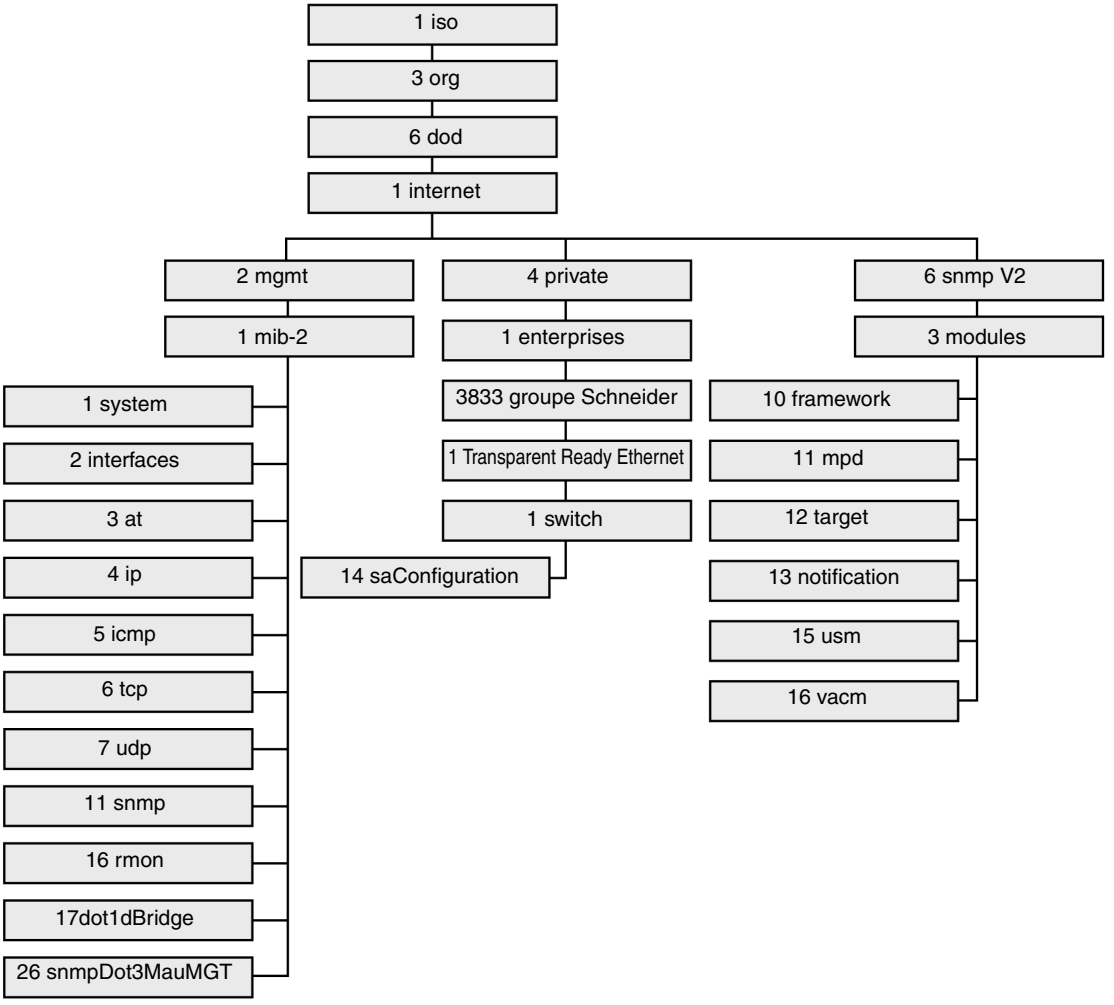
Syntax Definitions

The following table defines the syntax terms used in the MIB.

Term	Definition
Integer	an integer in the range 0-2^{32}
IP address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC address	12-digit hexadecimal number in accordance with ISO / IEC 8802-3
Object Identifier	x.x.x.x... (e.g., 1.3.6.1.1.4.1.3833...)
Octet String	ASCII character string
PSID	power supply identifier (power supply number)
Time Ticks	Stopwatch elapsed time (in seconds) = numerical value / 100 numerical value = integer in the range 0-2^{32}
Timeout	time value in hundredths of a second time value = integer in the range 0-2^{32}
Type Field	4-digit hexadecimal number in accordance with ISO / IEC 8802-3
Counter	Integer (0-2^{32}) whose value is incremented by 1 when certain events occur.

MIB Tree Structure

The following flowchart describes the tree structure of the ESM MIB.



Note: Not all devices support all object classes. The value **not supported** is given in response to a non-supported object class request. Any attempt to alter a non-supported object class produces the message **bad value**.

MIB II

System Group (1.3.6.1.2.1.1)

The system group is a required group for all systems. It contains system-related objects. If an agent has no value for a variable, then the response returned includes a string of length 0.

```
(1) system
    |-- (1) sysDescr
    |-- (2) sysObjectID
    |-- (3) sysUpTime
    |-- (4) sysContact
    |-- (5) sysName
    |-- (6) sysLocation
    |-- (7) sysServices
    |-- (8) sysORLastChange
    |-- (9) sysORTable
        |-- (1) sysOREntry
            |-- (1) sysORIndex
            |-- (2) sysORID
            |-- (3) sysDescr
            |-- (4) sysORUpTime
```

System Group Objects

The following table describes the member objects of the system group.

Object	OID	Syntax	Access	Description
sysDescr	1.3.6.1.2.1.1.1.0	ASCII String (Size: 0-255	Read	Is a verbal description of the entry. This value should contain the full name and version number of type of system hardware, operating system software, and network software. The description must consist only of printable ASCII characters.
sysObjectID	1.3.6.1.2.1.1.2.0	Object identifier	Read	Is the authorization identification of the manufacturer of the network management system that is integrated in this device. This value is placed in the SMI enterprises subtree (1.3.6.1.4.1) and describes which type of device is being managed. For example: if the manufacturer **Schneider Electric** is assigned the subtree 1.3.6.1.4.1.3833, then he can assign his switch the identifier 1.3.6.1.4.1.3833.1.1.
sysUpTime	1.3.6.1.2.1.1.3.0	Time ticks	Read	Is the time in 1/100 seconds since the last reset of the network management unit.
sysContact	1.3.6.1.2.1.1.4.0	ASCII string (size: 0-255)	Read and write	Is the clear-text identification of the contact person for this managed node along with the information about how that person is to be contacted.
sysName	1.3.6.1.2.1.1.5.0	ASCII string (size: 0-255)	Read and write	Is a name for this node for identifying it for administration. By convention, this is the fully qualified name in the domain.
sysLocation	1.3.6.1.2.1.1.6.0	ASCII string (size: 0-255)	Read and write	the physical location of this node (e.g., **staircase, 3rd floor**)
sysServices	1.3.6.1.2.1.1.7.0	Integer (0-127)	Read	This value indicates the services offered by the node. It is an integral value calculated by summing $2^{(layer - 1)}$ for each ISO layer for which the node provides service. For example: A node primarily provides routing functions (OSI layer 3): sysServices = $2^{(3-1)} = 4$ A node is a host and offers application and network services (OSI layers 4 and 7): sysServices = $2^{(4-1)} + 2^{(7-1)} = 72$

Interface Group (1.3.6.1.2.1.2)

The interface group contains information about the device interfaces.

```
(2) interfaces
    |-- (1) ifNumber
    |-- (2) ifTable
        |-- (1) ifEntry
            |-- (1) ifIndex
            |-- (2) ifDescr
            |-- (3) ifType
            |-- (4) ifMtu
            |-- (5) ifSpeed
            |-- (6) ifPhysAddress
            |-- (7) ifAdminStatus
            |-- (8) ifOperStatus
            |-- (9) ifLastChange
            |-- (10) ifInOctets
            |-- (11) ifInUcastPkts
            |-- (12) ifInNUcastPkts
            |-- (13) ifInDiscards
            |-- (14) ifInErrors
            |-- (15) ifInUnknownProtos
            |-- (16) ifOutOctets
            |-- (17) ifOutUcastPkts
            |-- (18) ifOutNUcastPkts
            |-- (19) ifOutDiscards
            |-- (20) ifOutErrors
            |-- (21) ifOutQLen
            |-- (22) ifSpecific
```

Address Translation Group (1.3.6.1.2.1.3)

The address translation group is required for all systems. It contains information about the assignment of addresses.

```
(3) at
    |-- (1) atTable
        |-- (1) atEntry
            |-- (1) atIfIndex
            |-- (2) atPhysAddress
            |-- (3) atNetAddress
```

Internet Protocol Group (1.3.6.1.2.1.4)

The internet protocol group is required for all systems. It contains information affecting IP switching.

```
(4) ip
    |-- (1) ipForwarding
    |-- (2) ipDefaultTTL
    |-- (3) ipInReceives
    |-- (4) ipInHdrErrors
    |-- (5) ipInAddrErrors
    |-- (6) ipForwDatagrams
    |-- (7) ipInUnknownProtos
    |-- (8) ipInDiscards
    |-- (9) ipInDelivers
    |-- (10) ipOutRequests
    |-- (11) ipOutDiscards
    |-- (12) ipOutNoRoutes
    |-- (13) ipReasmTimeout
    |-- (14) ipReasmReqds
    |-- (15) ipReasmOKs
    |-- (16) ipReasmFails
    |-- (17) ipFragOKs
    |-- (18) ipFragFails
    |-- (19) ipFragCreates
    |-- (20) ipAddrTable
    |   |-- (1) ipAddrEntry
            |-- (1) ipAdEntAddr
```

```
            |-- (2) ipAdEntIfIndex
            |-- (3) ipAdEntNetMask
            |-- (4) ipAdEntBcastAddr
            |-- (5) ipAdEntReasmMaxSize
    |-- (21) ipRouteTable
    |   |-- (1) ipRouteEntry
            |-- (1) ipRouteDest
            |-- (2) ipRouteIfIndex
            |-- (3) ipRouteMetric1
            |-- (4) ipRouteMetric2
            |-- (5) ipRouteMetric3
            |-- (6) ipRouteMetric4
            |-- (7) ipRouteNextHop
            |-- (8) ipRouteType
            |-- (9) ipRouteProto
            |-- (10) ipRouteAge
            |-- (11) ipRouteMask
            |-- (12) ipRouteMetric5
            |-- (13) ipRouteInfo
    |-- (22) ipNetToMediaTable
    |   |-- (1) ipNetToMediaEntry
    |       |-- (1) ipNetToMediaIfIndex
    |       |-- (2) ipNetToMediaPhysAddress
    |       |-- (3) ipNetToMediaNetAddress
    |       |-- (4) ipNetToMediaType
    |-- (23) ipRoutingDiscards
```

ICMP Group (1.3.6.1.2.1.5)

The internet control message protocol group is obligatory for all systems. It contains all the information on error handling and control for data exchange in the Internet.

```
(5) icmp
    |-- (1) icmpInMsgs
    |-- (2) icmpInMsgs
    |-- (3) icmpInDestUnreachs
    |-- (4) icmpInTimeExcds
    |-- (5) icmpInParmProbs
    |-- (6) icmpInSrcQuenchs
    |-- (7) icmpInRedirects
    |-- (8) icmpInEchos
    |-- (9) icmpInEchoReps
    |-- (10) icmpInTimestamps
    |-- (11) icmpInTimestampReps
    |-- (12) icmpInAddrMasks
    |-- (13) icmpInAddrMaskReps
    |-- (14) icmpOutMsgs
    |-- (15) icmpOutErrors
    |-- (16) icmpOutDestUnreachs
    |-- (17) icmpOutTimeExcds
    |-- (18) icmpOutParmProbs
    |-- (19) icmpOutSrcQuenchs
    |-- (20) icmpOutRedirects
    |-- (21) icmpOutEchos
    |-- (22) icmpOutEchoReps
    |-- (23) icmpOutTimestamps
    |-- (24) icmpOutTimestampReps
    |-- (25) icmpOutAddrMasks
    |-- (26) icmpOutAddrMaskReps
```

Transfer Control Protocol Group (1.3.6.1.2.1.6)

The transfer control protocol group is required for all systems that have implemented TCP. Instances of objects that describe information about a particular TCP connection exist only as long as the connection exists.

```
(6) tcp
    |-- (1) tcpRtoAlgorithm
    |-- (2) tcpRtoMin
    |-- (3) tcpRtoMax
    |-- (4) tcpMaxConn
    |-- (5) tcpActiveOpens
    |-- (6) tcpPassiveOpens
    |-- (7) tcpAttemptFails
    |-- (8) tcpEstabResets
    |-- (9) tcpCurrEstab
    |-- (10) tcpInSegs
    |-- (11) tcpOutSegs
    |-- (12) tcpRetransSegs
    |-- (13) tcpConnTable
    |   |-- (1) tcpConnEntry
    |       |-- (1) tcpConnState
    |       |-- (2) tcpConnLocalAddress
    |       |-- (3) tcpConnLocalPort
    |       |-- (4) tcpConnRemAddress
    |       |-- (5) tcpConnRemPort
    |-- (14) tcpInErrs
    |-- (15) tcpOutRsts
```

User Datagram Protocol Group (1.3.6.1.2.1.7)

The user datagram protocol group is required for all systems that have implemented UDP.

```
(7) udp
    |-- (1) udpInDatagrams
    |-- (2) udpNoPorts
    |-- (3) udpInErrors
    |-- (4) udpOutDatagrams
    |-- (5) udpTable
    |   |-- (1) udpEntry
    |       |-- (1) udpLocalAddress
    |       |-- (2) udpLocalPort
```

Simple Network Management Protocol Group (1.3.6.1.2.1.11)

The simple network management protocol group is required for all systems. In SNMP installations that have been optimized to support either just one agent or one management station, some of the listed objects will contain the value **O**

```
(11) snmp
    |-- (1) snmpInPkts
    |-- (2) snmpOutPkts
    |-- (3) snmpInBadVersions
    |-- (4) snmpInBadCommunityNames
    |-- (5) snmpInBadCommunityUses
    |-- (6) snmpInASNParseErrs
    |-- (7) not used
    |-- (8) snmpInTooBigs
    |-- (9) snmpInNoSuchNames
    |-- (10) snmpInBadValues
    |-- (11) snmpInReadOnlys
    |-- (12) snmpInGenErrs
    |-- (13) snmpInTotalReqVars
    |-- (14) snmpInTotalSetVars
    |-- (15) snmpInGetRequests
    |-- (16) snmpInGetNexts
    |-- (17) snmpInSetRequests
    |-- (18) snmpInGetResponses
```

```
|-- (19) snmpInTraps
|-- (20) snmpOutTooBigs
|-- (21) snmpOutNoSuchNames
|-- (22) snmpOutBadValues
|-- (23) not used
|-- (24) snmpOutGenErrs
|-- (25) snmpOutGetRequests
|-- (26) snmpOutGetNexts
|-- (27) snmpOutSetRequests
|-- (28) snmpOutGetResponses
|-- (29) snmpOutTraps
|-- (30) snmpEnableAuthenTraps
|-- (31) snmpSilentDrops
|-- (32) snmpProxyDrops
```

RMON Group (1.3.6.1.2.1.16)

This part of the MIB provides a continuous flow of current and historical network component data to the network management. The configuration of alarms and events controls the evaluation of network component counters. The agents inform the management station of the evaluation result by means of traps depending on the configuration.

```
(16 rmon
    |--(1) statistics
        |--(1) etherStatsTable
            |--(1) etherStatsEntry
                |--(1) etherStatsIndex
                |--(2) etherStatsDataSource
                |--(3) etherStatsDropEvents
                |--(4) etherStatsOctets
                |--(5) etherStatsPkts
                |--(6) etherStatsBroadcastPkts
                |--(7) etherStatsMulticastPkts
                |--(8) etherStatsCRCAlignErrors
                |--(9) etherStatsUndersizePkts
                |--(10) etherStatsOversizePkts
                |--(11) etherStatsFragments
```

```
                        |--(12) etherStatsJabbers
                        |--(13) etherStatsCollisions
                        |--(14) etherStatsPkts64Octets
                        |--(15) etherStatsPkts65to127Octets
                        |--(16) etherStatsPkts128to255Octets
                        |--(17) etherStatsPkts256to511Octets
                        |--(18) etherStatsPkts512to1023Octets
                        |--(19) etherStatsPkts1024to1518Octets
                        |--(20) etherStatsOwner
                        |--(21) etherStatsStatus
    |--(2) history
        |--(1) historyControlTable
            |--(1) historyControlEntry
                |--(1) historyControlIndex
                |--(2) historyControlDataSource
                |--(3) historyControlBucketsRequested
                |--(4) historyControlBucketsGranted
                |--(5) historyControlInterval
                |--(6) historyControlOwner
                |--(7) historyControlStatus
        |--(2) etherHistoryTable
            |--(1) etherHistoryEntry
                |--(1) etherHistoryIndex
                |--(2) etherHistorySampleIndex
                |--(3) etherHistoryIntervalStart
                |--(4) etherHistoryDropEvents
                |--(5) etherHistoryOctets
                |--(6) etherHistoryPkts
                |--(7) etherHistoryBroadcastPkts
                |--(8) etherHistoryMulticastPkts
                |--(9) etherHistoryCRCAlignErrors
                |--(10) etherHistoryUndersizePkts
                |--(11) etherHistoryOversizePkts
```

```
                |--(12) etherHistoryFragments
                |--(13) etherHistoryJabbers
                |--(14) etherHistoryCollisions
                |--(15) etherHistoryUtilization
    |--(3) alarm
        |--(1) alarmTable
            |--(1) alarmEntry
                |--(1) alarmIndex
                |--(2) alarmInterval
                |--(3) alarmVariable
                |--(4) alarmSampleType
                |--(5) alarmValue
                |--(6) alarmStartupAlarm
                |--(7) alarmRisingThreshold
                |--(8) alarmFallingThreshold
                |--(9) alarmRisingEventIndex
                |--(10) alarmFallingEventIndex
                |--(11) alarmOwner
                |--(12) alarmStatus
    |--(9) event
        |--(1) eventTable
            |--(1) eventEntry
                |--(1) eventIndex
                |--(2) eventDescription
                |--(3) eventType
                |--(4) eventCommunity
                |--(5) eventLastTimeSent
                |--(6) eventOwner
                |--(7) eventStatus
        |--(2) logTable
            |--(1) logEntry(1)
                |--(1) logEventIndex
                |--(2) logIndex
```

```
                |--(3) logTime
                |--(4) logDescription
    |--(19) probeConfig
        |--(15) smonCapabilities
    |--(22) switchRMON
            |--(1) smonMIBObjects
                |--(1) dataSourceCaps
                    |--(1) dataSourceCapsTable
                        |--(1) dataSourceCapsEntry
                            |--(1) dataSourceCapsObject
                            |--(2) dataSourceRmonCaps
                            |--(3) dataSourceCopyCaps
                            |--(4) dataSourceCapsIfIndex
                |--(3) portCopyConfig
                    |--(1) portCopyTable
                        |--(1) portCopyEntry
                            |--(1) portCopySource
                            |--(2) portCopyDest
                            |--(3) portCopyDestDropEvents
                            |--(4) portCopyDirection
                            |--(5) portCopyStatus
```

dot1dBridge (1.3.6.1.2.1.17)

This part of the MIB contains bridge-specific objects.

```
(17) dot1dBridge
    |--(1) dot1dBase
        |--(1) dot1dBaseBridgeAddress
        |--(2) dot1dBaseNumPorts
        |--(3) dot1dBaseType
        |--(4) dot1dBasePortTable
            |--(1) dot1dBasePortEntry
                |--(1) dot1dBasePort
                |--(2) dot1dBasePortIfIndex
                |--(3) dot1dBasePortCircuit
                |--(4) dot1dBasePortDelayExceededDiscards
```

```
                |--(5) dot1dBasePortMtuExceededDiscards
        |--(2) dot1dStp
            |--(1) dot1dStpProtocolSpecification
            |--(2) dot1dStpPriority
            |--(3) dot1dStpTimeSinceTopologyChange
            |--(4) dot1dStpTopChanges
            |--(5) dot1dStpDesignatedRoot
            |--(6) dot1dStpRootCost
            |--(7) dot1dStpRootPort
            |--(8) dot1dStpMaxAge
            |--(9) dot1dStpHelloTime
            |--(10) dot1dStpHoldTime
            |--(11) dot1dStpForwardDelay
            |--(12) dot1dStpBridgeMaxAge
            |--(13) dot1dStpBridgeHelloTime
            |--(14) dot1dStpBridgeForwardDelay
            |--(15) dot1dStpPortTable
                |--(1) dot1dStpPortEntry
                    |--(1) dot1dStpPort
                    |--(2) dot1dStpPortPriority
                    |--(3) dot1dStpPortState
                    |--(4) dot1dStpPortEnable
                    |--(5) dot1dStpPortPathCost
                    |--(6) dot1dStpPortDesignatedRoot
                    |--(7) dot1dStpPortDesignatedCost
                    |--(8) dot1dStpPortDesignatedBridge
                    |--(9) dot1dStpPortDesignatedPort
                    |--(10) dot1dStpPortForwardTransitions
                    |--(11) dot1dStpPortPathCost32
            |--(16) dot1dStpVersion
            |--(17) dot1dStpTxHoldCount
            |--(18) dot1dStpPathCostDefault
            |--(19) dot1dStpExtPortTable
```

```
            |--(1) dot1dStpExtPortEntry
                |--(1) dot1dStpPortProtocolMigration
                |--(2) dot1dStpPortAdminEdgePort
                |--(3) dot1dStpPortOperEdgePort
                |--(4) dot1dStpPortAdminPointToPoint
                |--(5) dot1dStpPortOperPointToPoint
                |--(6) dot1dStpPortAdminPathCost
    |--(3) dot1dSr
    |--(4) dot1dTp
        |--(1) dot1dTpLearnedEntryDiscards
        |--(2) dot1dTpAgingTime
        |--(3) dot1dTpFdbTable
            |--(1) dot1dTpFdbEntry
                |--(1) dot1dTpFdbAddress
                |--(2) dot1dTpFdbPort
                |--(3) dot1dTpFdbStatus
        |--(4) dot1dTpPortTable
            |--(1) dot1dTpPortEntry
                |--(1) dot1dTpPort
                |--(2) dot1dTpPortMaxInfo
                |--(3) dot1dTpPortInFrames
                |--(4) dot1dTpPortOutFrames
                |--(5) dot1dTpPortInDiscards
    |--(5) dot1dStatic
        |--(1) dot1dStaticTable
            |--(1) dot1dStaticEntry
                |--(1) dot1dStaticAddress
                |--(2) dot1dStaticReceivePort
                |--(3) dot1dStaticAllowedToGoTo
                |--(4)  dot1dStaticStatus
    |--(6) pBridgeMIB
        |--(1) pBridgeMIBObjects
            |--(1) dot1dExtBase
```

```
                    |--(1) dot1dDeviceCapabilities
                    |--(2) dot1dTrafficClassesEnabled
                    |--(3) dot1dGmrpStatus
                    |--(4) dot1dPortCapabilitiesTable
                        |--(1) dot1dPortCapabilitiesEntry
                            |--(1) dot1dPortCapabilities
                |--(2) dot1dPriority
                    |--(1) dot1dPortPriorityTable
                        |--(1) dot1dPortPriorityEntry
                            |--(1) dot1dPortDefaultUserPriority
                            |--(2) dot1dPortNumTrafficClasses
                    |--(3) dot1dTrafficClassTable
                        |--(1) dot1dPortPriorityEntry
                            |--(1) dot1dTrafficClassPriority
                            |--(2) dot1dTrafficClass
                |--(3) dot1dGarp
                    |--(1) dot1dPortGarpTable
                        |--(1) dot1dPortGarpEntry
                            |--(1) dot1dPortGarpJoinTime
                            |--(2) dot1dPortGarpLeaveTime
                            |--(3) dot1dPortGarpLeaveAllTime
                |--(4) dot1dGmrp
                    |--(1) dot1dPortGmrpTable
                        |--(1) dot1dPortGmrpEntry
                            |--(1) dot1dPortGmrpStatus
                          |--(2) dot1dPortGmrpFailedRegistrations
                            |--(3) dot1dPortGmrpLastPduOrigin
        |--(7) qBridgeMIB
            |--(1) qBridgeMIBObjects
                |--(1) dot1qBase
                    |--(1) dot1qVlanVersionNumber
                    |--(2) dot1qMaxVlanId
                    |--(3) dot1qMaxSupportedVlans
```

```
                        |--(4) dot1qNumVlans
                        |--(5) dot1qGvrpStatus
                    |--(2) dot1qTp
                        |--(1) dot1qFdbTable
                            |--(1) dot1qFdbEntry
                                |--(1) dot1qFdbId
                                |--(2) dot1qFdbDynamicCount
                            |--(2) dot1qTpFdbTable
                                |--(1) dot1qTpFdbEntry
                                    |--(1) dot1qTpFdbAddress
                                    |--(2) dot1qTpFdbPort
                                    |--(3) dot1qTpFdbStatus
                        |--(3) dot1qTpGroupTable
                            |--(1) dot1qTpGroupEntry
                                |--(1) dot1qTpGroupAddress
                                |--(2) dot1qTpGroupEgressPorts
                                |--(3) dot1qTpGroupLearnt
                        |--(4) dot1qForwardAllTable
                            |--(1) dot1qForwardAllEntry
                                |--(1) dot1qForwardAllPorts
                                |--(2) dot1qForwardAllStaticPorts
                                |--(3) dot1qForwardAllForbiddenPorts
                        |--(5) dot1qForwardUnregisteredTable
                            |--(1) dot1qForwardUnregisteredEntry
                                |--(1) dot1qForwardUnregisteredPorts
                               |--(2) dot1qForwardUnregisteredStaticPorts
                                |--(3)
dot1qForwardUnregisteredForbiddenPorts
                    |--(3) dot1qStatic
                        |--(1) dot1qStaticUnicastTable
                            |--(1) dot1qStaticUnicastEntry
                                |--(1) dot1qStaticUnicastAddress
                                |--(2) dot1qStaticUnicastReceivePort
                               |--(3) dot1qStaticUnicastAllowedToGoTo
```

```
                        |--(4) dot1qStaticUnicastStatus
                    |--(2) dot1qStaticMulticastTable
                        |--(1) dot1qStaticMulticastEntry
                            |--(1) dot1qStaticMulticastAddress
                            |--(2) dot1qStaticMulticastReceivePort
                            |--(3)
dot1qStaticMulticastStaticEgressPorts
                            |--(4)
dot1qStaticMulticastForbiddenEgressPorts
                            |--(5) dot1qStaticMulticastStatus
                |--(4) dot1qVlan
                    |--(1) dot1qVlanNumDeletes
                        |--(3) dot1qVlanStaticTable
                            |--(1) dot1qVlanStaticEntry
                                |--(1) dot1qVlanStaticName
                                |--(2) dot1qVlanStaticEgressPorts
                                |--(3) dot1qVlanForbiddenEgressPorts
                                |--(4) dot1qVlanStaticUntaggedPorts
                                |--(5) dot1qVlanStaticRowStatus
                    |--(5) dot1qPortVlanTable
                        |--(1) dot1qPortVlanEntry
                            |--(1) dot1qPvid
                            |--(2) dot1qPortAcceptableFrameTypes
                            |--(3) dot1qPortIngressFiltering
                            |--(4) dot1qPortGvrpStatus
                            |--(5) dot1qPortGvrpFailedRegistrations
                            |--(6) dot1qPortGvrpLastPduOrigin
```

MAU Management Group (1.3.6.1.2.1.26)

The MAU management group is responsible for setting the autonegotiation parameters.

```
(26) snmpDot3MauMgt
    |-- (2) dot3IfMauBasicGroup
    |   |-- (1) ifMauTable
    |       |-- (1) ifMauEntry
    |           |-- (1) ifMauIfIndex
    |           |-- (2) ifMauIndex
    |           |-- (3) ifMauType
    |           |-- (4) ifMauStatus
    |           |-- (5) ifMauMediaAvailable
    |           |-- (6) ifMauMediaAvailableStateExits
    |           |-- (7) ifMauJabberState
    |           |-- (8) ifMauJabberingStateEnters
    |           |-- (9) ifMauFalseCarriers
    |           |-- (10)ifMauTypeList
    |           |-- (11)ifMauDefaultType
    |           |-- (12)ifMauAutoNegSupported
    |-- (5) dot3IfMauAutoNegGroup
    |   |-- (1) ifMauAutoNegTable
    |       |-- (1) ifMauAutoNegEntry
    |           |-- (1) ifMauAutoNegAdminStatus
    |           |-- (2) ifMauAutoNegRemoteSignaling
    |           |-- (4) ifMauAutoNegConfig
    |           |-- (5) ifMauAutoNegCapability
    |           |-- (6) ifMauAutoNegCapAdvertised
    |           |-- (7) ifMauAutoNegCapReceived
    |           |-- (8) ifMauAutoNegRestart
```

Private MIB

Overview

The private MIB is for configuring the device-specific properties of the ESM. The groups below are implemented in the ESM from the private MIB saConfiguration (OID = 1.3.6.1.4.1.3833.1.1.14).

- saChassis (OID = 1.3.6.1.4.1.3833.1.1.14.1)
- saAgent (OID = 1.3.6.1.4.1.3833.1.1.14.2)
- saUserGroup (OID = 1.3.6.1.4.1.3833.1.1.14.3)
- saRingRedundancy (OID = 1.3.6.1.4.1.3833.1.1.14.5)
- saProducts (OID = 1.3.6.1.4.1.3833.1.1.14.10)

Device Group

The device group contains information on the status of the ESM hardware.

```
(14) saConfiguration
    |-- (1) saChassis
    |   |-- (1) saSystemTable
    |       |-- (1) saSysProduct
    |       |-- (2) saSysVersion
    |       |-- (3) saSysGroupCapacity
    |       |-- (4) saSysGroupMap
    |       |-- (5) saSysMaxPowerSupply
    |       |-- (6) saSysMaxFan
    |       |-- (7) saSysGroupModuleCapacity
    |       |-- (8) saSysModulePortCapacity
            |-- (9) saSysGroupTable
                |-- (1) saSysGroupEntry
                    |-- (1) saSysGroupID
                    |-- (2) saSysGroupType
                    |-- (3) saSysGroupDescription
                    |-- (4) saSysGroupHwVersion
                    |-- (5) saSysGroupSwVersion
                    |-- (6) saSysGroupModuleMap
                    |-- (7) saSysGroupAction
                    |-- (8) saSysGroupActionResult
            |-- (11) saInterfaceTable
```

```
                        |-- (1) saIfEntry
                           |-- (1) saIfaceGroupID
                           |-- (2) saIfaceID
                           |-- (3) saIfaceStpEnable
                           |-- (4) saIfaceLinkType
                           |-- (5) saIfaceAction
                           |-- (6) saIfaceNextHopMacAddress
                           |-- (7) saIfaceFlowControl
                           |-- (8) saIfacePriorityThreshold
                           |-- (9) saIfaceName
                           |-- (10) saIfaceTrunkID
                           |-- (11) saIfacePrioTOSEnable
                           |-- (12) saIfBcastLimit
                           |-- (13) saIfaceUtilization
                           |-- (14) saIfaceUtilizationControlInterval
                    |-- (20) saSysChassisName
                    |-- (21) saSysStpEnable
                    |-- (22) saSysFlowControl
                    |-- (23) saSysBOOTPEnable
                    |-- (24) saSysDHCPEnable
                    |-- (25) saSysTelnetEnable
                    |-- (26) saSysHTTPEnable
                    |-- (27) saSysPlugAndPlay
                    |-- (29) saBcastLimiterMode
                    |-- (30) saSystemTime
                |   |-- (2) saPSTable
                |       |-- (1) saPSEntry
                |           |-- (1) saPSSysID
                |           |-- (2) saPSID
                |           |-- (3) saPSState
                    |-- (5) saCurrentAddressTable
                        |-- (1) saCurrentAddressEntry
                            |-- (1) saCurrentAddress
```

```
                    |-- (2) saCurrentAddressReceivePort
                    |-- (3) saCurrentAddressStaticEgressPorts
                    |-- (4) saCurrentAddressEgressPorts
                    |-- (5) saCurrentAddressStatus
|   |-- (10) saESMext
|       |-- (1) saESMOperMode
|       |-- (2) saESMConfigError
|       |-- (3) saESMSigRelayState
|       |-- (4) saSigLinkTable
|           |-- (1) saSigLinkEntry
|               |-- (1) saSigLinkID
|               |-- (2) saSigLinkAlarm
        |-- (5) saSigTrapReason
        |-- (6) saSigReasonIndex
        |-- (7) saESMTopologyGroup
            |-- (1) saESMPartnerIpAddress
            |-- (2) saESMTopologyTable
                |-- (1) saESMTopologyEntry
                    |-- (1) saESMTopologyLinkID
                    |-- (2) saESMTopologyIpAddress
        |-- (9) saESMDisableLearningGroup
            |-- (1) saESMDisableLearningStatus
        |-- (10) saESMSigRelayGroup
            |-- (1) saESMSigRelayMode
            |-- (2) saESMSigRelayManualState
        |-- (11) saESMVlanGroup
            |-- (1) saESMVlanMode
            |-- (2) saESMVlanStatus
        |-- (12) saESMSelftestGroup
            |-- (1) saESMSelftestResult
            |-- (2) saESMSelftestMode
        |-- (13) saESMPSGroup
            |-- (1) saESMPSAlarm
```

Management Group

The management group contains parameters for configuring the management agent.

```
(14)saConfiguration
    |-- (2) saAgent
    |   |-- (1) saAction
    |   |-- (2) saActionResult
    |   |-- (3) saNetwork
    |       |-- (1) saNetLocalIPAddr
    |       |-- (2) saNetLocalPhysAddr
    |       |-- (3) saNetGatewayIPAddr
    |       |-- (4) saNetMask
            |-- (7) saNetAction
            |-- (8) saNetVlanID
            |-- (20) saNetEthernetSwitchConfigurationGroup
               |-- (1) saNetEthernetSwitchConfigurationStatus
            |-- (30) saNetSNTPGroup
                |-- (1) saNetSNTPStatus
                |-- (2) saNetSNTPServer
                |-- (3) saNetSNTPTime
                |-- (4) saNetSNTPLocalOffset
                |-- (5) saNetSNTPServer2
                |-- (6) saNetSNTPSyncInterval
                |-- (7) saNetSNTPAcceptBroadcasts
                |-- (8) saNetSNTPAnycastAddr
                |-- (9) saNetSNTPAnycastVlan
                |-- (10) saNetSNTPAnycastInterval
                |-- (11) saNetSNTPOperStatus
            |-- (50) saNetSNMPGroup
                |-- (1) saNetSNMPv1Status
                |-- (2) saNetSNMPv2Status
                |-- (3) saNetSNMPv3Status
                |-- (4) saNetSNMPAccessStatus
    |   |-- (4) saFSTable
```

```
|       |-- (1) saFSUpdFileName
|       |-- (2) saFSConfFileName
|       |-- (3) saFSLogFileName
|       |-- (4) saFSUserName
|       |-- (5) saFSTPPassword
|       |-- (6) saFSAction
|       |-- (8) saFSActionResult
        |-- (9) saFSBootConfiguration
        |-- (10) saFSRunningConfiguration
        |-- (200) saBackupConfigGroup
|           |-- (1) saBackupConfigAdapterStatus
|   |-- (5) saTempTable
|       |-- (1) saTemperature
|       |-- (2) saTempUprLimit
|       |-- (3) saTempLwrLimit
|   |-- (7) saAuthGroup
|       |-- (1) saAuthHostTableEntriesMax
|       |-- (2) saAuthCommTableEntriesMax
|       |-- (3) saAuthCommTable
|           |-- (1) saAuthCommEntry
|               |-- (1) saAuthCommIndex
|               |-- (2) saAuthCommName
|               |-- (3) saAuthCommPerm
|               |-- (4) saAuthCommState
|       |-- (4) saAuthHostTable
|           |-- (1) saAuthHostEntry
|               |-- (1) saAuthHostIndex
|               |-- (2) saAuthHostName
|               |-- (3) saAuthHostCommIndex
|               |-- (4) saAuthHostIpAddress
|               |-- (5) saAuthHostIpMask
|               |-- (6) saAuthHostState
|   |-- (8) saTrapGroup
```

```
|       |-- (1) saTrapCommTableEntriesMax
|       |-- (2) saTrapDestTableEntriesMax
|       |-- (3) saTrapCommTable
|           |-- (1) saTrapCommEntry
|               |-- (1) saTrapCommIndex
|               |-- (2) saTrapCommCommIndex
|               |-- (3) saTrapCommColdStart
|               |-- (4) saTrapCommLinkDown
|               |-- (5) saTrapCommLinkUp
|               |-- (6) saTrapCommAuthentication
|               |-- (7) saTrapCommBridge
|               |-- (8) saTrapCommRMON
|               |-- (9) saTrapCommUsergroup
|               |-- (10)saTrapCommDualHoming
|               |-- (11)saTrapCommChassis
|               |-- (12)saTrapCommState
|       |-- (4) saTrapDestTable
|           |-- (1) saTrapDestEntry
|               |-- (1) saTrapDestIndex
|               |-- (2) saTrapDestName
|               |-- (3) saTrapDestCommIndex
|               |-- (4) saTrapDestIpAddress
|               |-- (5) saTrapDestIpMask
|               |-- (6) saTrapDestState
|   |-- (9) saLastAccessGroup
|       |-- (1) saLastIpAddr
|       |-- (2) saLastPort
|       |-- (3) saLastCommunity
|   |-- (10) saMulticast
|     |-- (1) saIGMPGroup
|       |-- (2) saIGMPSnoop
|         |-- (1) saIGMPSnoopStatus
|         |-- (2) saIGMPSnoopUnknownMode
```

```
|          |-- (3) saIGMPSnoopAgingTime
|          |-- (10) saIGMPSnoopQueryTable
|          |   |-- (1) saIGMPSnoopQueryEntry
|          |   |   |-- (1) saIGMPSnoopQueryVlanIndex
|          |   |   |-- (2) saIGMPSnoopQueryPorts
|          |-- (11) saIGMPSnoopFilterTable
|          |   |-- (1) saIGMPSnoopFilterEntry
|          |   |   |-- (1) saIGMPSnoopFilterVlanIndex
|          |   |   |-- (2) saIGMPSnoopFilterAddress
|          |   |   |-- (3) saIGMPSnoopFilterLearntPorts
|          |-- (12) saIGMPSnoopForwardAllTable
|          |   |-- (1) saIGMPSnoopForwardAllEntry
|          |   |   |-- (1) saIGMPSnoopForwardAllVlanIndex
|          |   |   |-- (2) saIGMPSnoopForwardAllStaticPorts
|          |-- (13) saIGMPSnoopQueryStaticTable
|          |   |-- (1) saIGMPSnoopQueryStaticEntry
|          |   |   |-- (1) saIGMPSnoopQueryStaticVlanIndex
|          |   |   |-- (2) saIGMPSnoopQueryStaticPorts
|          |-- (100) saIGMPQuerierGroup
|          |   |-- (1) saIGMPQuerierStatus
|          |   |-- (2) saIGMPQuerierMode
|          |   |-- (3) saIGMPQuerierTransmitInterval
|          |   |-- (4) saIGMPQuerierMaxResponseTime
|          |   |-- (5) saIGMPQuerierProtocolVersion
|   |-- (11) saRelayGroup
|       |-- (1) saRelayOption82Status
|       |-- (2) saRelayOptionRemoteIDType
|       |-- (3) saRelayOptionRemoteID
|       |-- (10) saRelayServerGroup
|           |-- (1) saRelayDHCPServerIpAddr
|           |-- (2) saRelayDHCPServer2IpAddr
|           |-- (3) saRelayDHCPServer3IpAddr
|           |-- (4) saRelayDHCPServer4IpAddr
```

```
|       |-- (11) saRelayInterfaceTable
|           |-- (1) saRelayIfEntry
|               |-- (1) saRelayIfaceGroupID
|               |-- (2) saRelayIfaceID
|               |-- (3) saRelayIfaceOption82Enable
|               |-- (4) saRelayIfaceBCRequestFwd
|       |-- (20) saRelayBCPktInCnt
|       |-- (21) saRelayMCPktInCnt
|       |-- (22) saRelayPktServerRelayCnt
|       |-- (23) saRelayPktClientRelayCnt
|       |-- (24) saRelayErrCnt
|       |-- (25) saRelayLastDuplicateIP
```

User Groups Group

The user groups group contains parameters for configuring the user group functions.

```
(14) saConfiguration
    |-- (3) saUserGroup
        |-- (4) saPortSecurityTable
            |-- (1) saPortSecurityEntry
                |-- (1) saPortSecSlotID
                |-- (2) saPortSecPortID
                |-- (3) saPortSecPermission
                |-- (4) saPortSecAllowedUserID
                |-- (5) saPortSecAllowedGroupIDs
                |-- (6) saPortSecConnectedUserID
                |-- (7) saPortSecAction
                |-- (8) saPortSecAutoReconfigure
```

Redundancy Group

The redundancy group contains parameters for configuring the redundancy functions.

```
(14) saConfiguration
    |-- (5) saRingRedundancy
        |-- (1) saRingRedTable
            |-- (1) saRingRedEntry
                |-- (1) saRingRedPrimGroupID
```

```
                    |-- (2) saRingRedPrimIfIndex
                    |-- (3) saRingRedPrimIfOpState
                    |-- (4) saRingRedRedGroupID
                    |-- (5) saRingRedRedIfIndex
                    |-- (6) saRingRedRedIfOpState
                    |-- (7) saRingRedOperState
                    |-- (8) saRingRedMode
                    |-- (9) saRingRedConfigOperState
            |-- (2) saRingCouplingTable
                |-- (1) saRingCouplingEntry
                    |-- (1) saRingCplInterconnGroupID
                    |-- (2) saRingCplInterconnIfIndex
                    |-- (3) saRingCplInterconnIfOpState
                    |-- (4) saRingCplControlGroupID
                    |-- (5) saRingCplControlIfIndex
                    |-- (6) saRingCplControlIfOpState
                    |-- (7) saRingCplControlMode
                    |-- (8) saRingCplPartnerIpAddr
                    |-- (9) saRingCplPartnerInterconnGroupID
                    |-- (10) saRingCplPartnerInterconnIfIndex
                    |-- (11) saRingCplPartnerInterconnIfOpState
                    |-- (12) saRingCplOperState
                    |-- (13) saRingCplMode
                    |-- (14) saRingCplRowStatus
                    |-- (15) saRingCplConfigOperState
                    |-- (16) saRingCplCouplingLinks
    |-- (10) saProducts
        |-- (2) ESMx7100
```

SNMP V2 Module MIB

Overview

The SNMP V2 Module MIB is based on the SNMP MIB (Simple Network Management Protocol Group).

Framework Group

The framework group contains parameters for describing SNMP Management Frameworks.

```
(3) snmpModules
    |-- (10) snmpFrameworkMIB
    |   |-- (2) snmpFrameworkMIBObjects
    |       |-- (1) snmpEngine
    |           |-- (1) snmpEngineID
    |           |-- (2) snmpEngineBoots
    |           |-- (3) snmpEngineTime
    |           |-- (4) snmpEngineMaxMessageSize
```

MPD Group

The MPD group (Message Processing and Dispatching) contains parameters for dispatching SNMP messages which are potentially in different SNMP versions. It defines the procedures for dispatching potentially multiple versions of SNMP messages.

```
    |-- (3) snmpModules
    |   |-- (11) snmpMPDMIB
    |       |-- (2) snmpMPDMIBObjects
    |           |-- (1) snmpUnknownSecurityModels
    |           |-- (2) snmpInvalidMsgs
    |           |-- (3) snmpUnknownPDUHandlers
```

Target Group

The Target group contains parameters for specifying targets of SNMP management operations.

```
|-- (3) snmpModules
|   |-- (12) snmpTargetMIB
|       |-- (2) snmpTargetObjects
|           |-- (1) snmpTargetSpinLock
|               |-- (2) snmpTargetAddrTable
|                   |-- (1) snmpTargetAddrEntry
|                       |-- (1) snmpTargetAddrName
|                       |-- (2) snmpTargetAddrTDomain
|                       |-- (3) snmpTargetAddrTAddress
|                       |-- (4) snmpTargetAddrTimeout
|                       |-- (5) snmpTargetAddrRetryCount
|                       |-- (6) snmpTargetAddrTagList
|                       |-- (7) snmpTargetAddrParams
|                       |-- (8) snmpTargetAddrStorageType
|                       |-- (9) snmpTargetAddrRowStatus
|            |-- (3) snmpTargetParamsTable
|               |-- (1) snmpTargetParamsEntry
|                  |-- (1) snmpTargetParamsName
|                  |-- (2) snmpTargetParamsMPModel
|                  |-- (3) snmpTargetParamsSecurityModel
|                  |-- (4) snmpTargetParamsSecurityName
|                  |-- (5) snmpTargetParamsSecurityLevel
|                  |-- (6) snmpTargetParamsStorageType
|                  |-- (7) snmpTargetParamsRowStatus
|             |-- (4) snmpUnavailableContexts
|             |-- (5) snmpUnknownContexts
```

Notification Group

The Notification group contains parameters for specifying targets for notification filtering.

```
(3) snmpModules
|-- (13) snmpNotificationMIB
|   |-- (1) snmpNotifyObjects
|       |-- (1) snmpNotifyTable
|           |-- (1) snmpNotifyEntry
|               |-- (1) snmpNotifyName
|               |-- (2) snmpNotifyTag
|               |-- (3) snmpNotifyType
|               |-- (4) snmpNotifyStorageType
|               |-- (5) snmpNotifyRowStatus
|           |-- (2) snmpNotifyFilterProfileTable
|               |-- (1) snmpNotifyFilterProfileEntry
|                   |-- (1) snmpNotifyFilterProfileName
|                   |-- (2) snmpNotifyFilterProfileStorType
|                   |-- (3) snmpNotifyFilterProfileRowStatus
|           |-- (3) snmpNotifyFilterTable
|               |-- (1) snmpNotifyFilterEntry
|                   |-- (1) snmpNotifyFilterSubtree
|                   |-- (2) snmpNotifyFilterMask
|                   |-- (3) snmpNotifyFilterType
|                   |-- (4) snmpNotifyFilterStorageType
|                   |-- (5) snmpNotifyFilterRowStatus
```

USM Group

The USM group (User-Based Security Model) defines the elements of procedure for providing SNMP message level security.

```
(3) snmpModules
| |-- (15) snmpUsmMIB
|   |-- (1) usmMIBObjects
|       |-- (1) usmStats
|           |-- (1) usmStatsUnsupportedSecLevels
|           |-- (2) usmStatsNotInTimeWindows
|           |-- (3) usmStatsUnknownUserNames
```

```
|           |-- (4) usmStatsUnknownEngineIDs
|           |-- (5) usmStatsWrongDigests
|           |-- (6) usmStatsDecryptionErrors
|       |-- (2) usmUser
|           |-- (1) usmUserSpinLock
|               |-- (2) usmUserTable
|                   |-- (1) usmUserEntry
|                       |-- (1) usmUserEngineID
|                       |-- (2) usmUserName
|                       |-- (3) usmUserSecurityName
|                       |-- (4) usmUserCloneFrom
|                       |-- (5) usmUserAuthProtocol
|                       |-- (6) usmUserAuthKeyChange
|                       |-- (7) usmUserOwnAuthKeyChange
|                       |-- (8) usmUserPrivProtocol
|                       |-- (9) usmUserPrivKeyChange
|                       |-- (10) usmUserOwnPrivKeyChange
|                       |-- (11) usmUserPublic
|                       |-- (12) usmUserStorageType
|                       |-- (13) usmUserStatus
```

VACM Group

The VACM group (View-based Access Control Model) defines the elements of procedure for controlling access to management information.

```
(3) snmpModules
| |-- (16) snmpVacmMIB
|   |-- (1) vacmMIBObjects
|       |-- (1) vacmContextTable
|           |-- (1) vacmContextEntry
|               |-- (1) vacmContextName
|           |-- (2) vacmSecurityToGroupTable
|               |-- (1) vacmSecurityToGroupEntry
|                   |-- (1) vacmSecurityModel
|                   |-- (2) vacmSecurityName
|                   |-- (3) vacmGroupName
```

```
|                    |-- (4) vacmSecurityToGroupStorageType
|                    |-- (5) vacmSecurityToGroupStatus
|            |-- (4) vacmAccessTable
|                |-- (1) vacmAccessEntry
|                    |-- (1) vacmAccessContextPrefix
|                    |-- (2) vacmAccessSecurityModel
|                    |-- (3) vacmAccessSecurityLevel
|                    |-- (4) vacmAccessContextMatch
|                    |-- (5) vacmAccessReadViewName
|                    |-- (6) vacmAccessWriteViewName
|                    |-- (7) vacmAccessNotifyViewName
|                    |-- (8) vacmAccessStorageType
|                    |-- (9) vacmAccessStatus
|            |-- (5) vacmMIBViews
|                |-- (1) vacmViewSpinLock
|                |-- (2) vacmViewTreeFamilyTable
|                    |-- (1) vacmViewTreeFamilyEntry
|                        |-- (1) vacmViewTreeFamilyViewName
|                        |-- (2) vacmViewTreeFamilySubtree
|                        |-- (3) vacmViewTreeFamilyMask
|                        |-- (4) vacmViewTreeFamilyType
|                        |-- (5) vacmViewTreeFamilyStorageType
|                        |-- (6) vacmViewTreeFamilyStatus
```

RFCs

List of RFCs

The following table contains a list of RFCs:

RFC 768 (UDP)
RFC 783 (TFTP)
RFC 791 (IP)
RFC 792 (ICMP)
RFC 793 (TCP)
RFC 826 (ARP)
RFC 854 (Telnet)
RFC 855 (Telnet Option)
RFC 951 (BOOTP)
RFC 1112 (IGMPv1)
RFC 1155 (SMIv1)
RFC 1157 (SNMPv1)
RFC 1212 (Concise MIB Definitions)
RFC 1213 (MIB2)
RFC 1493 (Dot1d)
RFC 1542 (BOOTP Extensions)
RFC 1643 (Ethernet-Like MIB)
RFC 1757 (RMON)
RFC 1769 (SNTP)
RFC 1867 (HTML/2.0 Forms W/File Upload Extensions)
RFC 1901 (Community-Based SNMP v2)
RFC 1905 (Protocol Operations for SNMP v2)
RFC 1906 (Transport Mappings for SNMP v2)
RFC 1907 (MIB2)
RFC 1908 (Coexistence Between SNMP v1 and SNMP v2)
RFC 1945 (HTTP/1.0)
RFC 2068 (HTTP/1.1)
RFC 2131 (DHCP)
RFC 2132 (DHCP Options)
RFC 2233 (The Interface Group MIB Using SMI v2)
RFC 2236 (IGMPv2)

RFC 2239 (MAU MIB)
RFC 2246 (The TLs Protocol, Version 1.0)
RFC 2271 (SNMP Framework MIB)
RFC 2346 (AES Ciphersuites for Transport Layer Security)
RFC 2570 (Introduction to SNMP v3)
RFC 2571 (SNMP Framework)
RFC 2572 (SNMP MPD)
RFC 2573 (SNMP Applications)
RFC 2574 (SNMP USM)
RFC 2575 (SNMP VACM)
RFC 2576 (Coexistence Between SNMP v1, v2 and v3)
RFC 2578 (SMI v2)
RFC 2579 (Textual Conventions for SMI v2)
RFC 2580 (Conformance Statements for SMI v2)
RFC 2613 (SMON)
RFC 2618 (RADIUS Authentication Client MIB)
RFC 2620 (RADIUS Accounting MIB)
RFC 2674 (Dot1p/Q)
RFC 2818 (HTTP over TLs)
RFC 2851 (Internet Addresses MIB)
RFC 2865 (RADIUS Client)
RFC 2866 (RADIUS Accounting)
RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)
RFC 2869 (RADIUS Extensions)
RFC 2869 (RADIUS Support for EAP)
RFC 2933 (IGMP MIB)

IEEE Standards

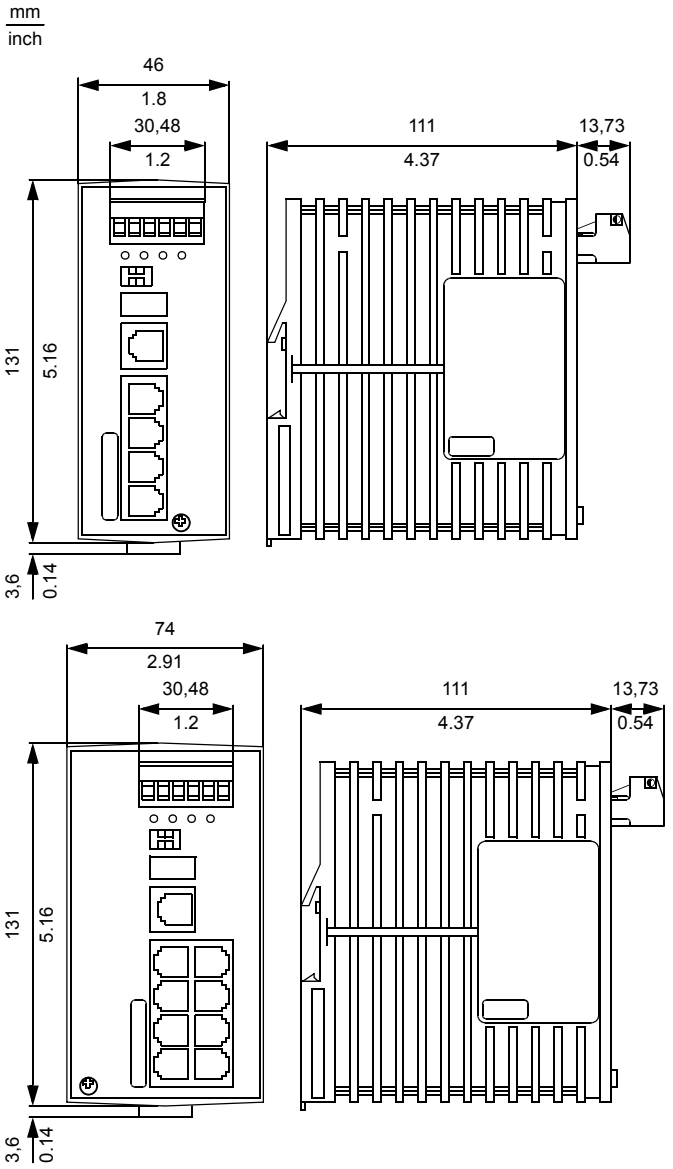
List of IEEE Standards

The following table lists the IEEE standards applying to the ESM.

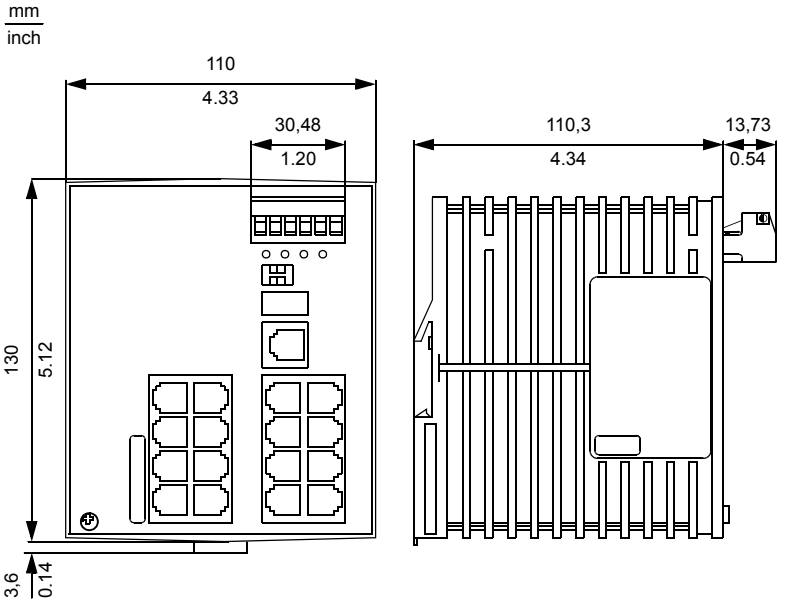
Standard	Explanation
IEEE 802.1 D	Switching, GARP, GMRP, Spanning Tree (supported via 802.1S implementation
IEEE 802.1 D-1998	Media Access Control (MAC) bridges (includes IEEE 802.1p Priority Dynamic and Multicast Filtering, GARP, GMRP)
IEEE 802.1 Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, port-based VLANs, GVRP)
IEEE 802.1 S	Multiple Spanning Tree
IEEE 802.1 v	Protocol-Based VLANs
IEEE 802.1 w.2001	Rapid Reconfiguration, supported via 802.1S implementation
IEEE 802.1 X	Port Authentication
IEEE 802.3 - 2002	Ethernet
IEEE 802.3 ac	VLAN Tagging
IEEE 802.3 ad	Link Aggregation with static LAG and LACP Support
IEEE 802.1 X	Port Authentication
IEEE 802.3 x	Flow Control

Dimension Drawings

4 and 8 Port Versions



16 and 24 Port Versions



General Technical Software Data

ESM

The following table shows the technical data of the ESM.

Switch	Data
Latency - 1000 MBit/s	 max. 3.5 µs
- 100 MBit/s	max. 4.5 µs
- 100 MBit/s	max. 19 µs
MAC address table	up to 8000 entries
Static Address Filter	up to 100 entries (in RM (redundancy manager) mode: 0 unicast entries

VLAN

The following table shows the VLAN-related technical data of the ESM.

VLAN	Data
VLAN ID	1 to 4062
Number of VLANs	max. 256 simultaneously per switch
Number of VLANs	max. 256 simultaneously per port
Number of VLANs with GMRP (VLAN 1)	max. 256 simultaneously per switch
Number of VLANs with GMRP (VLAN 1)	max. 256 simultaneously per port

Switches and Accessories

Scope of Delivery

The delivery comprises:

- selected switch version
- terminal block for supply voltage and signal contact
- description and manuals
- CD ROM

Order Numbers

Part Number		Description
4 Port Version	TCSESM043F23F0	4 10/100 TX Managed
	TCSESM043F1CU0	3 10/100 TX 1 100 FX-MM Managed
	TCSESM043F2CU0	2 10/100 TX 2 100 FX-MM Managed
	TCSESM043F1CS0	3 10/100 TX 1 100 FX-SM Managed
	TCSESM043F2CS0	2 10/100 TX 2 100 FX-SM Managed
8 Port Version	TCSESM083F23F0	8 10/100 TX Managed
	TCSESM083F1CU0	7 10/100 TX 1 100 FX-MM Managed
	TCSESM083F2CU0	6 10/100 TX 2 100 FX-MM Managed
	TCSESM083F1CS0	7 10/100 TX 1 100 FX-SM Managed
	TCSESM083F2CS0	6 10/100 TX 2 100 FX-SM Managed
	TCSESM083F2CX0	6 10/100 TX 1 100 FX-MM 1 100 FX-SM Managed
16 Port Version	TCSESM163F23F0	16 10/100 TX Managed
	TCSESM163F2CU0	14 10/100 TX 2 100 FX-MM Managed
24 Port Version	TCSESM243F2CU0	22 10/100 TX 2 100 FX-MM Managed
Gigabit - 10 Port Version	TCSESM103F23G0	8 10/100 TX 2 10/100/1000 TX Managed
	TCSESM103F2LG0	8 10/100 TX 2 1000 SFP (fiber) Managed **Note:** These products ship with open sockets (SFP) on the fiber ports, so in order to use these ports, you must order 1, or 2, media modules shown below.
Fiber Media Modules	TCSEAAF1LFU00	SFP-SX/LC fiber module for Gigabit
	TCSEAAF1LFS00	SFP-LX/LC fiber module for Gigabit
	TCSEAAF1LFH00	SFP-LH/LC fiber module for Gigabit
Accessories	TCSEAM0100	Memory Backup Adapter

Copyright for Integrated Software

GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can re-link them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the **Lesser** General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a **work based on the library** and a **work that uses the library**. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

Terms and Conditions

Terms and conditions for copying, distribution, and modification are listed in this topical discussion.

0—This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called **this License**). Each licensee is addressed as **you**.

A **library** means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The **library** below refers to any such software library or work that has been distributed under these terms. A **work based on the Library** means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term **modification**.)

Source code for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1—You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2—You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

(a) The modified work must itself be a software library.

(b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

(c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

(d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3—You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4—You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5—A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a **work that uses the LIbrary**. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a **work that uses the Library** with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a **work that uses the library**. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a **work that uses the library** uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6—As an exception to the Sections above, you may also combine or link a **work that uses the Library** with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

(a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable **work that uses the Library** as object code and/or source code, so that the user can modify the Library and then re-link to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.).

(b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

(c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

(d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

(e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the **work that uses the Library** must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7—You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

(a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the sections above.

(b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8—You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9—You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10—Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11—If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12—If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13—The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and **any later version** you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14—If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

No Warranty

15—BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY **AS IS** WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16—IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Applying These Terms

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the **copyright** line and a pointer to where the full notice is found.

```
<one line to give the library's name and a brief idea of what
it does.> Copyright (C) <year> <name of author>
```

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Also add information on how to contact you by electronic and paper mail. You should also get your employer (if you work as a programmer) or your school, if any, to sign a **copyright disclaimer** for the library, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James
Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice
```

That's all there is to it!

The Legion Of The Bouncy Castle

Switch Function Examples

B

At a Glance

Overview

This chapter provides two examples illustrating key ESM switch functions.

What's in this Chapter?

This chapter contains the following topics:

Setting Up the DHCP Server for Option 82

Introduction

⚠ WARNING

UNINTENDED OPERATION

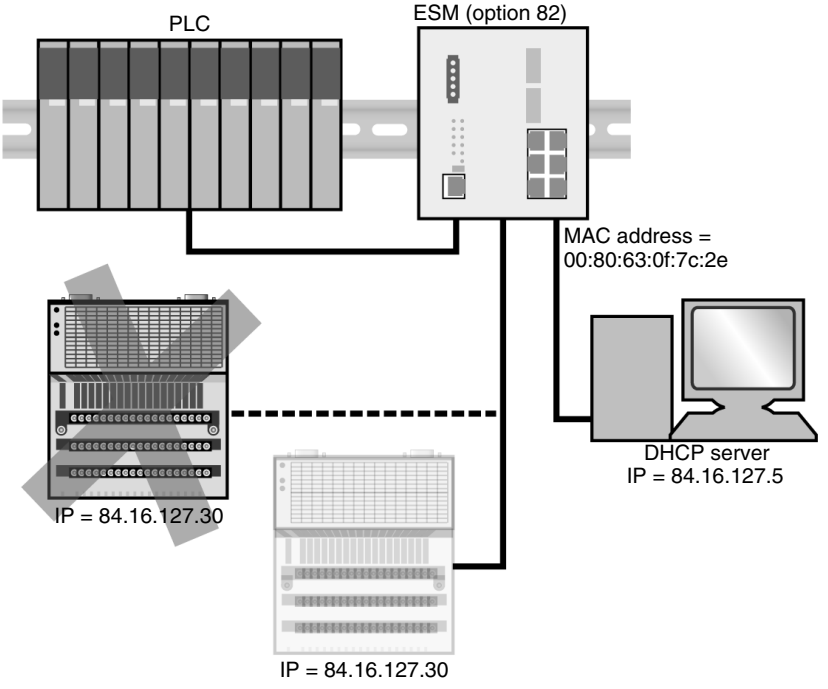
If IP addresses are assigned using DHCP option 82, changing the port to which a device is connected will cause its IP address to change.

- Do not change device port connections on the ESM.
- When performing maintenance on an ESM, make sure to label each Ethernet cable with the ESM port number assigned so that you can reestablish the same configuration.

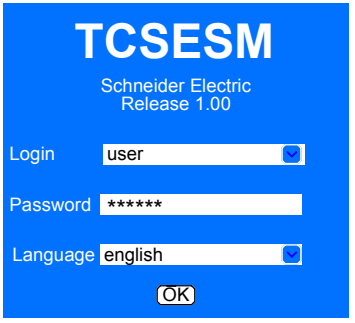
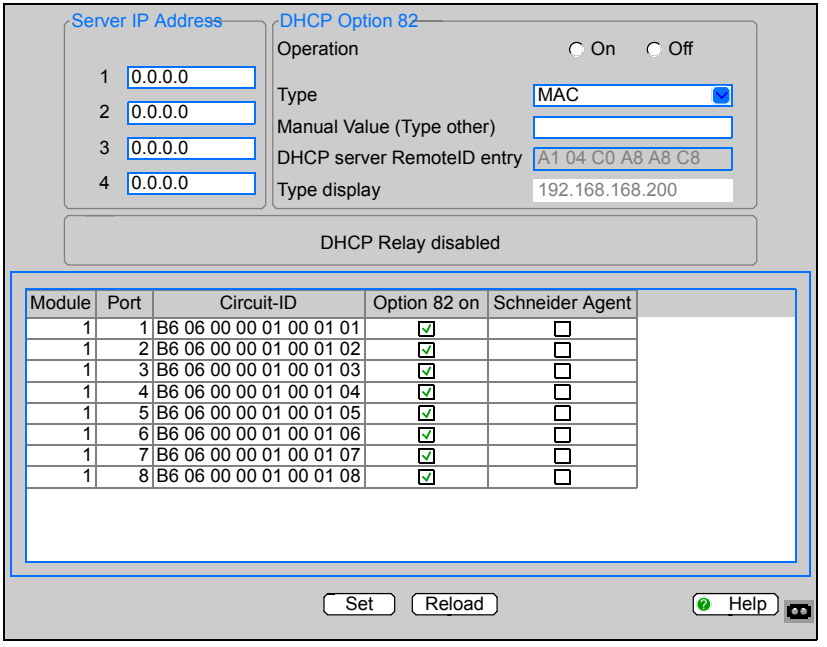
Failure to follow this instruction can result in death, serious injury, or equipment damage.

Option 82 Application Example

DHCP option 82 allows you to assign the same IP address to any device connected to a particular switch port. The server shown in the example below must support option 82.



Configuring a Switch for DHCP Option 82

Step	Action
1	Log in to the Web-based interface (see *p. 16*). 
2	Go to **Advanced** → **DHCP Relay Agent**. 
3	In line **1** of the **Server IP Address** group box, enter the DHCP server's IP address.
4	In the **Operation** line of the **DHCP Option 82** group box, select **On**.
5	Choose **MAC** from the drop-down list in the **Type** line.
6	Click **Set** to save the configuration.

DHCP Option 82 Server Hardware Address

DHCP option 82 servers require that you input a hardware address. This address consists of the switch's remote ID and circuit ID. The circuit ID identifies the port on the switch where the device to which you want to assign an IP address is connected.

The addresses of remote ID and circuit ID are shown on the DHCP Relay Agent web page, which is shown in step 2 of the procedure above. In the screen above, the remote ID is `A104C0A8A8C8`. If the device is connected to port 7 of the switch, then the circuit ID is `B606000001000107`.

Note: One tool you may use to set up DHCP server option 82 on your PC is haneWIN, which can be downloaded from the www.hanewin.de website. You may elect to use other appropriate software, like those included with Windows 2000 servers or Linux operating systems.
The haneWIN software can be tested for 30 calendar days from the date of the first installation before deciding whether you want to purchase a license. Schneider Electric does not guarantee in any way that the product will function as described and disclaims any responsibility for damages that may result from its use.

TFTP Server for Software Updates

Switch Software

The ESM software is in the flash memory by default. The ESM boots the software from the flash memory.

Software updates can be realized via a tftp server. This presupposes that a tftp server has been installed in the connected network and that it is active.

Note: An alternative to the tftp update is the http update. If you perform an http update you do not have to configure the tftp server.

The ESM requires the following information for updating software from the tftp server:

- its own IP address (entered permanently),
- the IP address of the tftp server or gateway to the tftp server,
- the path in which the operating system of the tftp server is located.

File transfer between the ESM and the tftp server is handled by way of the Trivial File Transfer Protocol (tftp).

Management station and tftp server may be made up of one or more computers.

Preparation of the tftp server for the ESM software involves:

- setting up the ESM directories and copying ESM software,
- setting up the tftp process.

Prerequisites for Setting Up the TFTP Process

The general prerequisites for setting up the tftp process are the following:

- The ESM knows its local IP address and the IP address of tftp server/gateway.
- The TCP/IP stack and tftp are installed on the tftp server.

Setting up the TFTP Process

The following table shows the steps for setting up the tftp process, with subsequent tables providing a breakdown according to operating system and application.

Step	Action	Comment
1	Check if the tftp daemon (background process) is running.	Check whether the file `etc/inetd.conf` contains the following line: • in SunOS `tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -s /tftpboot`, • in HP tftp dgram udp wait root /usr/etc/in.tftpd tftpd.
2	Check whether the status of this process is **IW**.	The status should be **IW**.
3	If the process is not in the file, or if the related line is commented out (#), modify `etc/inetd.conf` accordingly.	
4	Enter the UNIX command `man tftp`.	

The command `ps` does not always show the tftp daemon, although it is actually running.

Tftp Installation on HP Workstations

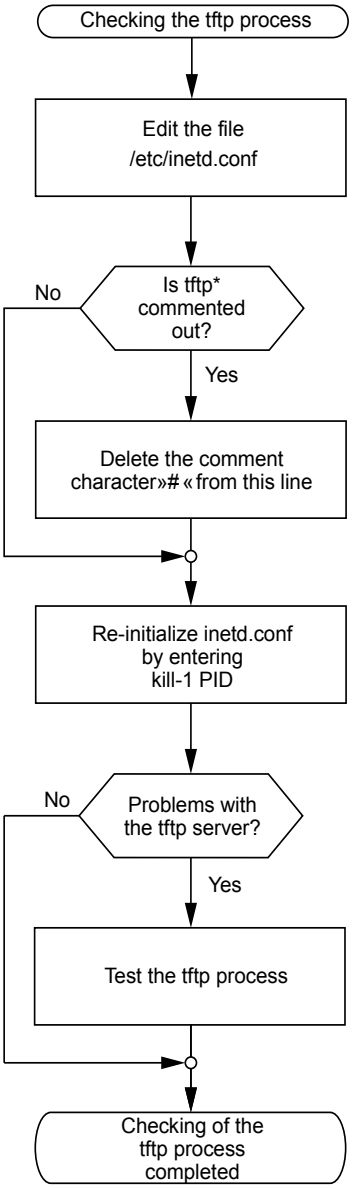
The following table describes the special steps to be taken when installing tftp on HP workstations.

Step	Action	Comment
1	Enter the user tftp in the file `/etc/passwd`.	For example: *tftp*:*:*510*:*20*:*tftp server*:/usr/tftpdir:*/bin/false* Where: *tftp* = user ID * = in the password field *510* = sample user ID *20* = sample group ID *tftp server* = reely selectable designation */bin/false* = mandatory entry (login shell).

2	Test the tftp process.	For example:
		`cd /tftpboot/ESM`
		`tftp <tftp-Servername>`
		`get ESM/ESM.bin`
		`rm ESM.bin`.

Flowchart for Setup

The following flowchart summarizes the procedure for setting up the tftp server with SunOS and HP.



e.g.,
cd /tftpboot/ESM
tftp <tftp-Servername>
get ESM/ESM.bin

Response if the process is running: Received...

rm ESM.bin

* tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot

Software Access Rights

The agent needs read permission to the tftp directory with the ESM software.

Directory Structure of the Software

The following table shows the directory structure of the tftp server with stated access rights, once the ESM software has been installed.

Filename	Access
TCSESM.xxxxx.bin	444-r--r--r-

d = directory; r = read; w = write; x = execute

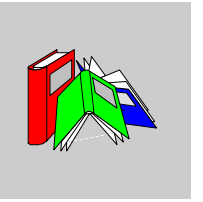
1st position designates d (directory)

2nd to 4th positions designate access rights of user

5th to 7th positions designate access rights of user groups

8th to 10th positions designate access rights of all others.

Glossary



E

EAM The EAM (Memory back up adapter) is a USB device which stores the configuration data of the ESM switch. If the switch fails, the configuration data can be easily transferred to another switch.

F

FDB The forwarding database stores addresses (which may be MAC addresses or network addresses) against the relevant forwarding data (i.e. port numbers).

G

GARP GARP (General Attribute Registration Protocol) is a standard for registering a client station into a multicast domain. GARP is an industry-standard protocol defined by IEEE 802.1P.

GMRP GMRP (GARP Multicast Registration Protocol) is a General Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility. GMRP is an industry-standard protocol defined by IEEE 802.1P.

I

ICMP ICMP (Internet Control Message Protocol) is TCP/IP protocol used to send error and control messages. For example, a router uses ICMP to notify the sender that its destination node is not available.

IGMP IGMP (Internet Group Management Protocol) governs the management of multicast groups in a TCP/IP network.

L

LLDP The LLDP (Link Layer Discovery Protocol) provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to neighboring devices that store the data in a MIB (management information base).

N

NTP NTP (Network Time Protocol) is used to update the real time clock in a computer. There are numerous primary and secondary servers in the Internet that are synchronized to the international time standard Coordinated Universal Time (UTC) via radio, satellite or modem.

R

RFC RFC (Request For Comment) is document that describes the specifications for a recommended technology. RFCs are used by the Internet Engineering Task Force (IETF) and other standards bodies.

RM RM (Redundancy Manager) is a switch function which allows you to close both ends of a backbone in a line-type configuration to create a redundant HIPER ring.

RSTP RSTP (Rapid Spanning Tree protocol) provides a loop free topology for any LAN (Local Area Network) or bridged network.

S

SFP The SFP interface (Small Form Factor Pluggable interface) is an industry standard daughter card used in networking. Their main advantage is that new speeds can be interfaced to an expensive network device by changing only the SFP module.

T

TFTP The TFTP (Trivial Transfer File Protocol) is a version of the TCP/IP FTP protocol that has no directory or password capability.

V

VLAN VLANs (Virtual Local Area Networks) are logical subgroups within a local area network that is created via software rather than manually moving cables in the wiring closet.

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W